情報システム ユーザガイドライン

正しい利用と管理のために

User's Guidelines

はじめに

インターネットの普及で色々な情報を簡単に手に入れたり発信したりできるようになりました。 しかし、その一方では様々な問題が生まれています。悪意をもった利用者からの攻撃やコンピュータウィルスによる脅威はもちろん、場合によっては無意識のうちに加害者となってしまうこともあります。

本ガイドラインでは、インターネット社会の中で被害者にも加害者にもならないための注意事項を説明します。

また、社会問題となっているにもかかわらず、ソフトウェア（コンピュータプログラム）の不正コピーや、Winny 等のファイル交換ソフトを利用した違法流通等による、著作権侵害に関する事件の発生が後を絶たず、また、その損害額は年々上昇傾向にあります。もし、私たちが著作権侵害を起こした場合、その個人及び組織は刑事罰と民事責任を負うことになります。

「ソフトウェアライセンス」では、ソフトウェアの正しい利用と管理を促すことを目的とし、基本的事項を平易に記載したものであり、「共通編」と「管理編」の2部構成となっています。

「共通編」では、学生の皆さんと一般教職員の皆さんを対象に、日常の学校内外での生活において、ソフトウェアを利用する際に留意すべき事項まとめています。 また、「管理編」では、ソフトウェアの管理を担当されている教職員の皆さんを対象に、ライセンス管理台帳やインストール管理台帳の整備・運用等、ソフトウェアの適切な管理を実現するために、取り組むべき事項をまとめています。

目次

情報セキュリティ入門

1. インターネットと情報セキュリティ対策

（1）インターネットの発展と現状

インターネットは、もともと大学や研究所をつなぐ学術用ネットワークとして発展してきました。

しかし、今では、企業間のビジネスや個人でも幅広く利用されています。パソコンおよびネットワーク接続費用の低価格化により、インターネット利用人口はどんどん増えています。自宅でインターネットを使っている人は、日本人のおよそ75％（2009年4月総務省調査による）に達していると言われています。

（2）インターネットに潜む危険性

インターネットは日本人にとって“普通”の道具になりつつありますが、その危険性を十分理解していない人も多いようです。いくつかの事例を見てみましょう。

ネットワークからの脅威

- コンピュータウィルスつきの電子メールをうっかり開いてしまい、ウィルスに感染した。
- 不正にコンピュータが侵入され、ホームページが書き換えられてしまった。
- 顧客や学生の個人情報がインターネット上に流出した。
- サービス利用不能攻撃（ DoS攻撃）によってネットワークが停止した。
- パスワードや銀行口座の暗証番号などが盗聴されてしまった。

「コンピュータウィルスに感染したことに気付かずにウィルスつきのメールや迷惑メールを他人に送付してしまった。」という事例も数多く報告されています。被害者のはずが、気がつかないうちに加害者となってしまい、その責任を問われることもあります。この場合、「ウィルスに感染していることを知らなかった。」といっても通用しません。

インターネットに流れる情報と責任

インターネットに流れる情報は、その通信路上で容易に盗み見ることが可能です。十分注意していないと、前記のように、個人情報が流出したり、パスワードや銀行口座の暗証番号が盗まれてしまったりします。一方、インターネットの最大の特徴は匿名性（誰が利用しているのかわからない、という性質）であると言われていますが、サーバ上のアクセス記録から接続したコンピュータを特定することが可能です。インターネット上の行動に責任を持つようにしましょう。

(3)自己防衛の重要性と方法

このような危険から自分自身を守ろうとすることが「情報セキュリティ対策」の出発点になります。このためには、個人個人の意識の向上と自己防衛の姿勢が重要です。

自己防衛について重要な事柄を少しだけ説明しておきましょう。

自己防衛に必要なこと(1)

学校で指定するアンチウィルスソフトウェア(ウィルス対策ソフトウェア)を必ず導入すること。また、アンチウィルスソフトウェアのウィルス定義ファイルを常に最新にして、定期的にウィルスチェックをすること。

アンチウィルスソフトウェアには有料のものから無料のものまでいろいろありますが、各高専でサイトライセンスを取得している場合が多いと思われます。多くの場合はキャンパス内の利用に限り自由にインストール可能です。(詳しくは各高専の情報セキュリティ推進委員長、情報処理センター等に問い合わせて下さい。)学校で使うパソコンには必ずインストールしてください。学生・教職員の皆さんが私有するパソコンについても市販のアンチウィルスソフトを各自でインストールして下さい。

[解説1]無料のアンチウィルスソフト

AVG、Avast!といった無料のアンチウィルスソフトウェアも存在しています。市販のアンチウィルスソフトウェアから一部の機能を制限したもので、ウィルスの発見・駆除能力はほぼ同等と言われています。ただし、ライセンス条件から利用の制限(個人所有の1台に限りインストールが可能)がありますので、よく確認しましょう。また、無料のアンチウィルスソフトウェアそのものにウィルスが含まれている事例もあります。信頼のおけないものはインストールしないようにしましょう。

自己防衛に必要なこと(2)

オペレーティングシステムやブラウザ、電子メール、オフィス等のソフトウェア更新を、怠らずに実施すること。

オペレーティングシステムやウェブブラウザなどは、セキュリティ上何らかの欠陥を含んでいるものです。その欠陥のために、外部から見えてはいけない情報が見えてしまったり、本来出来ないはずの操作が出来てしまったりして、情報が漏れたり外部の人に自分のパソコンを勝手に操作されてしまったりということが生じます。このような欠陥を「セキュリティホール」と呼びます。メーカーはセキュリティホールが分かり次第改善していますので、Microsoft Update などを活用してオペレーティングシステムやオフィスソフトウェアを最新の状態にしておくように心がけてください。また、電子メールを扱うメールソフト[注1]やウェブブラウザについても随時更新して下さい。さらに、

- ・Adobe Acrobat Reader/Acrobat
- ・Adobe Flash Player
- ・Oracle JRE(旧 Sun JRE)
- ・Quick Time

等も最新のバージョンにしておかないと、悪意のある Web サイトを閲覧しただけでコンピュータウィルスに感染する場合があります。最新のバージョンかどうかを確認し、適宜バージョンアップを実施しましょう。(なお、MyJVN というソフトウェアで最新のバージョンを確認できますので必要に応じて利用して下さい。http://jvndb.jvn.jp/apis/myjvn/vccheckhelp.html)

[注1]メールソフトとは、メールサーバを経由して電子メールを送受信するためのソフトウェアを指します。
たとえば、ウェブブラウザ機能の拡張版である Microsoft 社の Windows Mail(旧 Outlook Express)、
オープンソースの Thunderbird、独立したソフトウェアである Beckey など多くのものがあります。

自己防衛に必要なこと(3)

開発元がはっきりしない怪しいソフトウェアの導入はしないこと。P2Pファイル共有ソフトウェアは使わないこと。

信頼できないソフトウェアを導入すると、システムを破壊するコンピュータウィルスが含まれているケースがあります。また、キー入力したパスワードや銀行口座番号、暗証番号などの情報を第三者に送信するスパイウェアと呼ばれるコンピュータウィルスが隠されているケースもあります。 P2Pファイル共有ソフトウェアについては、後で詳しく説明します。

自己防衛に必要なこと(4)

懸賞サイト、無料ゲームサイトなどで不用意に自分のメールアドレスを登録しないこと。

これらのサイトでは、懸賞や無料ゲームを利用してメールアドレスの収集を行っているケースがあります。その結果、コンピュータウィルスを含む迷惑メールが大量に送付されて来ることになります。信頼できないサイトは利用しないようにしましょう。

(4)情報セキュリティ対策

インターネットの危険性から自分自身を守ることが重要だと述べました。同じように学校や会社も組織として自分自身を守る必要があります。このように、情報社会における危険から自分自身を守ることを情報セキュリティの確保と言い、そのための対策を「情報セキュリティ対策」と呼びます。

国立高等専門学校機構では、情報セキュリティ対策における基本的な考え方を「情報セキュリティポリシー基本方針」、基本方針を実行するための体制、組織および運用方法の大枠を「情報セキュリティポリシー対策規則」として定めています。さらに、この2つの規則に基づいて、各高専で「情報セキュリティ管理規程」、「情報セキュリティ推進規程」、「情報セキュリティ教職員規程」、「情報セキュリティ利用者規程」などが定められています。

各高専の情報セキュリティ対策は校長が責任者となって実行に移されますが、すべての事項を直接監

督することは出来ません。そこで、事項ごとに直接監督する教職員を決めています。たとえば、情報センターにある情報演習室やパソコンについてはセンター担当の技術職員、研究室のパソコンについては研究室の教員というようになっています。このガイドラインは、そのような人を一般的に「管理者」と呼び、特に重要な場合には上記の「情報セキュリティ管理規程」で定めている職名を付記します。

国立高等専門学校機構はたくさんの**情報資産**を持っています。それらすべてを同じように守ろうとすると、手間や経費が膨大なものになってしまいます。そこで、「情報セキュリティ格付規則」により、情報を**機密性、完全性及び可用性**の観点から分類して、取り扱いを決めています。 情報の中で、特に注意して扱わなければならないものを**要保護情報**と呼んでいます。

[解説2]情報資産とは？

> 情報資産とは、情報システムと情報そのものを言います。ただし、**情報システム**とは、情報処理及び情報ネットワークに係わるシステムのことで、「コンピュータシステム」、「情報ネットワーク」、「情報ネットワーク機器」及び「ソフトウェア」を含みます。

[解説3]機密性、完全性、可用性とは？

> 機密性とは、「秘密にする必要がある」という性質で、機密性が一番高い情報（これを**機密性3情報**と言います）の例として「実施前の入学試験問題」があります。完全性とは「改ざんや誤り、破損、紛失等によって利用者の権利が著しく侵害される又は学校の活動に重大な支障が出る」という性質で、完全性が高い情報（これを**完全性2情報**と言います）の例として「学籍簿に記録された成績」が挙げられます。可用性とは「無くなったり利用不可能になったりしたら利用者の権利が著しく侵害される又は学校の活動に重大な支障が出る」という性質で、可用性が高い情報（これを**可用性2情報**と言います）の例としては入学試験の日時や場所が挙げられます。機密性については「機密性3情報ほどではないが漏洩したらやっぱり困る」という情報として**機密性2情報**という分類があります。機密性3情報と機密性2情報をまとめて**機密情報**と呼びます。

[解説4]要保護情報とは？

> 学校が持っている情報のなかで、とくに注意して取り扱わなければならないものを「要保護情報」と呼びます。要保護情報には、「絶対秘密にしなければならない情報（**機密性3情報**）」と、間違いのない状態でいつでも利用できるようにしておかなければならない情報（**完全性2かつ可用性2**である情報）」の2つのパターンがあります。第1のパターンの例としては、学生の成績や住所などが挙げられます。ブログや掲示板で同級生の成績や住所などを勝手に公開してはいけません。第2のパターンの例としては、学校のホームページ上で公開されている入試情報があります。もしも、ホームページ上の入試情報などが書き換えられているのを見付けたら直ちに通報して下さい。（→第5章参照）

2. ユーザIDとパスワードの管理

(1)ユーザIDとパスワード、漏れるとどうなる？

みなさんには、入学時に学内の情報システムを利用する際に用いるユーザ ID(学生番号)とパスワードを付与しています。このユーザIDとパスワードが第三者に知られてしまうとどのようなことが起きてしまうのでしょうか？

ユーザ ID とパスワードが第三者に知られるとどうなるか？

- **自分宛ての電子メールや自分に関するデータが盗み読みされてしまいます。**
- **自分が知らないうちにデータが追加されたり、改ざん(または破壊)されたりします。**
- **自分になりすました第三者によって不正なアクセスが行われ、身に覚えがないのに犯人にされてしまいます。**

以上のように自分自身が不利益を受けるだけはありません。一人のユーザIDやパスワードが漏れると、他の人のユーザIDやパスワードを知る手がかりになってしまうこともあります。その結果、学校全体のセキュリティレベルを下げてしまいますので、ユーザIDとパスワードの管理は非常に重要です[注2]。また逆に、他人のユーザ ID やパスワードを不正な形で利用(不正アクセス[注3])してはいけません。

[注2]残念ながら、ユーザIDがメールアドレスの中に現れてしまう高専もあります。このような場合には特に、パスワードを第三者に知られないようにすることが重要になってきます。

[注3]不正アクセスとは、利用の許可を与えられていない利用者が、情報システムを利用したり、データの読み書きを行うことを指します。たとえば、インターネット上のオンラインゲームで、他人のユーザIDとパスワードを用いて他人になりすます行為などが該当します。

(2)管理上の注意事項

ユーザ ID とパスワードについての一般的注意事項

- **入学時に付与された初期パスワードを速やかに変更すること。**
- **定期的にパスワードを変更すること。**
- **他人のユーザIDやパスワードを使用しないこと。**
- **他人に自分のユーザIDやパスワードを教えないこと。**

- **メモ、紙、付せんにパスワードを書かないこと。(他人の目に触れるところにパスワードを記入した付せんを貼る行為は「パスワードを無効にすること」と同じです。)**
- **パソコンを利用する際にパスワード入力を要求するように設定すること。また、自分のパソコンを他人に使わせる場合でも、他人にパスワードを教えずに自分自身でログインを行うこと。**
- **パスワードを容易に推測されないものにすること。**
- **ネットワーク上で入力を要求されるパスワード(ネットワーク認証システム、インターネット上の各種会員ページ)についても上記と同様な扱いを行うこと。学校などのパスワードと同じにしないこと。**

一部の高専では学生証と職員証を IC カード化していますが、この IC カード内にも皆さんの身分を証明するための情報(識別コード)が記録されています。この学生証または職員証を利用することで、校舎への入退館システム、各種証明書発行などのサービスが利用可能となっています。学生証及び職員証は皆さんの身分を証明するもので、情報システムにおけるユーザ ID 及びパスワードと同等の意味を持ちます。つぎの注意事項を守って下さい。

学生証や職員証の取り扱いにも注意して下さい!

- **学生証や職員証を放置する行為は厳禁。盗難等にも気をつけること。**
- **他者に使わせたり貸したりしないこと。**
- **利用する必要がなくなった場合は遅滞なく学校へ返還すること。**
- **紛失した場合は速やかに学校へ届け出ること。**

(3)パスワードの作り方

安全のため皆さんには初期パスワードを付与していますが、速やかに自分独自のパスワードに変更して下さい。一般的に利用可能な文字は英字(大文字、小文字は区別されます)、数字、記号です。また、変更する際に覚えにくいパスワードを作ると、結果として「紙に書く」という行為につながってしまいますので、「推測されにくく、しかも覚えやすいパスワード」というのが基本となります。

まず、良くないパスワードを紹介します。数字のみ、辞書に載っている英単語、生年月日、名前(自分や著名人の名前)のアルファベットなどは推測され易いので使わないで下さい。

良くないパスワードの例

◆	19800123	生年月日（免許証などから容易に推測されてしまいます！）
◆	Yamadataro	自分の名前（こちらも容易に推測されてしまいます！）
◆	Internet	辞書に載っている英単語そのもの（英文辞書を使った侵入ツールが公開されており、場合によっては短時間で破られます。）
◆	Password1	辞書の単語＋数字（特に、この password1 というパスワードは、インターネット上の不正侵入に関するパスワード収集でナンバーワンになったそうです。）

［解説5］パスワードの強さを測るには？

　マイクロソフト社などで、パスワードの強度を測定するサイト（パスワードチェッカー、パスワード強度チェッカーなど）がいくつか公開されています。また、自分が利用しているパスワードがどれぐらいの時間で見破られてしまうか、ということをチェックしてくれるサイトもあります。普段何気なしに利用しているパスワードについても注意を払って下さい。
https://www.microsoft.com/japan/protect/yourself/password/checker.mspx

　パスワードの作成方法については、いろいろな方法が紹介されていますが、基本的には「英字（大文字、小文字の双方を含める）、数字、記号をすべて利用すること」がポイントとなります。また、覚えやすく第三者に推測されにくい、ということも大切な要素となります。良くないパスワードの例で紹介しましたが、英単語をそのまま使わない場合であっても、「英単語の前後に記号や数字を続けるだけ」、「英単語の a を@に置き換えるだけ」などの単純な変更も危険なので注意しましょう。安全性を考慮した上で、皆さん自身が工夫して安全なパスワードを作成しましょう[注4]。

［注4］ほとんどの高専で8文字以上のパスワード長が利用できますが、パスワード長に制限がある高専もあるので、各自確認して下さい。

高専統一パスワードポリシー

◆ パスワードの最小文字数　：8文字
◆ パスワードの必須文字種　：以下の文字種を強制的に各1文字以上含める
　英字（大文字／A～Z）、英字（小文字／a～z）、数字（0～9）
◆ パスワードの有効期限　：400日以内　（継続利用できる期間）
◆ パスワードの履歴　：1世代以上　（パスワード再利用禁止の世代数）

3. パソコンの取り扱い

この章ではパソコンの取り扱いについての注意事項を述べます。中には第 2 章ですでに注意した事柄もありますが、全体をまとめる意味で再記しておきます。なお、これらの多くはワークステーションや大型計算機といったコンピューター一般にあてはまる事柄です。

さて、高専の施設・設備（具体的にはコンピュータやネットワークのことです。）は高専の活動のために備えられているものですから、当然、個人の趣味や商取引などに使うことは許されません。これを明確にするために、以下では「学校の業務[注5]目的以外の使用を禁止する。」というような表現で、注意を喚起しています。必ず守って下さい。

［注5］**学校の業務**とは、教育、研究、社会貢献、国際交流等の目的で、学校として行う事項を指します。
学生については、勉学、研究、クラブ活動などで教員の指示の下に、または教員の許可を得て行う事項です。

（1）PCワーキングエリア内でのパソコンの利用

まず、 PC ワーキングエリア（情報処理センター、CAD演習室、マルチメディア演習室などパソコンを使った授業・演習等を行うための部屋のことです。具体的には各高専で定めます。）で禁止している事項を示します。

PC ワーキングエリア内での一般的禁止事項

- **PC ワーキングエリア内での飲食。ただし、管理者が許可をした場合を除く。**
- **大声で騒ぐこと、ゴミを放置すること。**
- **未使用プリンタ用紙の持ち帰り、授業・実験等に関係しない私的なデータの印刷。**
- **空調コントローラの操作。ただし、管理者が許可した場合を除く。**

PC ワーキングエリア内に設置されたパソコンに関する禁止事項

- **機器のケーブル・コネクタを引き抜いたり、機器を持ち出したりすること。（無断で機器の接続を変更しないで下さい。）**

- **USB メモリを乱雑に引抜いたり、キーボードの乱打、機器の開口部に異物を詰め込むなど、機器の破損につながる行為をすること。（校内の機器一般について、取扱いはていねいに行って下さい。）**
- **パソコン本体にアプリケーションをインストールすること。ただし、管理者が許可した場合を除く。（不必要なソフトウェアのインストールはウィルス感染などの危険性を招きます。）**
- **使用後にパソコンの電源を切らずに放置すること。（利用が終わったらパソコンの電源を切って下さい。）**
- **パソコンをロックせずに長時間離席すること。（トイレなどで離席する場合もロックして下さい。）**
- **長時間に渡る端末の占有。ただし、授業等で教員から指示された場合を除く。**

（2）校内でパソコンを利用する場合

まず、外部からパソコン（学生・教員個人のものや外部の団体などのもの）を持ち込んで学校のネットワークに接続する場合には、以下の注意事項を厳守して下さい。

外部から持ち込んだパソコンを学校のネットワークに接続する際の注意事項

- **学校のネットワーク管理者（情報セキュリティ推進責任者）に申し出て許可を受けること。**
- **ネットワークに接続する前に、ウィルスやスパイウェア等、有害なソフトウェアが含まれていないことを確認すること。**

なお、具体的な許可手順については、各校のルールあるいは学校のネットワーク管理者の指示に従って下さい。たとえば、パソコンのネットワークインターフェースの物理アドレス（ MAC アドレス）と所有者の登録作業、簡単な申請による利用許可などの手順が考えられます。

次に、学校が保有・管理するパソコンを利用する場合、及び上記の許可を得て学校のネットワークに接続したパソコンを使用する場合に禁止している事項を示します。

学校が保有するパソコン及び学校のネットワークに接続されたパソコンに関する禁止事項

- **学校の業務に必要とされない作業を行うこと。（私的な電子メールの送受信やウェブの利用も禁止です。）**
- **学校の業務に必要とされないソフトウェアをインストールすること。（ゲームソフトは禁止）**
- **学校が定めたアンチウィルスソフトウェアを導入せずにパソコンを作動させること。（なお、パソコ**

ンに OS そのものを新たに導入する場合やアップグレードする場合は、可能な限り速やかにアンチウィルスソフトウェアを導入して下さい。また、Linux などの UNIX 系OS、MacOS などのアンチウィルスソフトウェアについては、別途学校の指示に従って下さい。）

- **使用しようとするソフトウェアの利用許諾条件（ライセンス）に反する行為を行うこと。（たとえば、購入ライセンス数を超えた不正コピー等は厳禁です。）**
- **ウィルスやスパイウェア等の有害ソフトウェアが含まれていないことを確認せずにソフトウェアをインストールすること、及び出所が定かでないソフトウェアをインストールすること。（新たなソフトウェアが必要になった場合は、必ずアンチウィルスソフトウェア等により安全性を確認した上でインストールして下さい。）**
- **ネットワーク帯域を占有してしまうような大量データの送受信など、ネットワークや情報システムに過度な負荷をかけて円滑な利用を妨げること。（気づかないうちにコンピュータウィルスが同様なことを行ってしまう場合があります。定期的にウィルスチェックを行って下さい。）**
- **著作権侵害を目的として、P2P ファイル共有ソフトウェアをインストールすること、及びそれを利用すること。**

高専機構では、著作権侵害を引き起こす可能性がある状態での**P2P ファイル共有ソフトウェア**の利用を禁止します。高専によっては **P2P ファイル共有ソフトウェア**の利用が発覚した場合、著作権侵害の有無を問わず厳重注意、停学等の処分を実施する場合があります。ただし、教育・研究などのために管理者（情報セキュリティ副責任者及び情報セキュリティ推進責任者）が特別に許可した場合は除きます。

［解説6］P2P ファイル共有ソフトウェアとは？

Winny、BitTorrent、Kazaa、Share、Cabos、Napster など、インターネットを通じてファイルを不特定多数のユーザで共有するために作られたソフトウェアです。別名「ファイル交換ソフト」とも言われます。 BitTorrent などは、 Linux などのソフトウェア配布で利用される場合があり、正しい目的で利用する場合は便利で高速なサービスとなります。しかし、ほとんどの場合、「著作権保護されたデータを違法に入手する。」ことを目的に利用されています。著作権侵害の目的では「絶対に使わない」のが当然ですが、それ以外の目的で使用する場合も、著作権侵害を引き起こす可能性がないか常に十分注意を払うことが必要です。高専によっては、著作権侵害の有無にかかわらず利用そのものを処罰の対象とする場合があります。

著作権侵害はエンジニアとして恥ずべき行為です

2010 年の著作権法の改正（データを提供するだけでなく、ダウンロードして入手することそのものが摘発の対象となった。）もあり、コンピュータを利用した著作権侵害行為について、警察や著作権保護団体による監視、摘発が強化されようとしています。エンジニアは知的財産権を産みだし、守るのが仕事です。そのエンジニアの卵が「著作権侵害」では、学校そのものの存在意義が問われます。

（3）自らが管理するパソコン

個人所有あるいは実験室等で管理を任せられているパソコンについては、つぎのような情報セキュリティ対策を実施して下さい。

自らが管理するパソコンについて実施すべき情報セキュリティ対策

- **利用しているコンピュータ OS の「セキュリティアップデート」（ WindowsUpdate など）を定期的に実行し、セキュリティホールを狙った攻撃（ウィルス感染や侵入）を防止すること。**
- **学校が指定する有料あるいは無料のアンチウィルスソフトウェアを導入すること。ただし、Linux のような UNIX 系OSや MacOS などに関するアンチウィルスソフトウェアについては、別途学校の指示に従うこと。**
- **アンチウィルスソフトウェアのウィルス定義ファイルを常に最新の状態に保つこと。**
- **アンチウィルスソフトウェアによって、定期的にパソコン内のファイルや USB メモリのファイルをチェックすること。**
- **実験室等で管理するパソコンは、認証なしでパソコンを使用できないようにすること。**
- **無線 LAN 等、盗聴される危険性のある通信経路を利用する場合には、暗号化により内容が解析できないようにすること。**
- **出所の定かでないソフトウェアをインストール、使用しないこと。**

（4）コンピュータウィルスとそのタイプ

コンピュータウィルスとは、コンピュータに被害をもたらす不正なプログラムの総称です。コンピュータウィルスはおおむね以下のように分類できます。

コンピュータウィルスとその種類

◆ **プログラムファイル感染型**

.exe、.com などの実行プログラムに感染するタイプ。

◆ **システムプログラム感染型**

Windows などの OS に含まれる実行プログラムに感染するタイプ。

◆ **マクロ型**

Microsoft 社の表計算ソフト Excel などに含まれるマクロプログラムに感染するタイプ。

◆ **Java・ActiveX 型**

ブラウザを利用する際にパソコンに取り込まれるプログラムを経由して感染するタイプ。

◆ **ワーム型**
電子メールなど、ネットワークを介して広がるタイプ。短期間で被害が拡大する。

◆ **トロイの木馬型（スパイウェア）**
パソコン上で取り扱うデータ、入力されたユーザ ID やパスワード、暗証番号等を第三者へ送信するタイプ。

◆ **USB メモリ型**
USB メモリを接続した際に自動的に開く機能（自動的に実行されるプログラム）を悪用して感染するタイプ。（他のウィルスをダウンロードするなどの機能を持ち、近年流行しています。）

運悪くウィルスに感染してしまったときの対処方法

- **ネットワークケーブルのコネクターを切り離し（無線LANの場合は、無線LAN用のユニットを取りはずすか、電源を切る。）、管理者に連絡する。**
- **管理者の指示に従い、アンチウィルスソフトウェアのウィルス定義ファイルを最新のものに更新する。**
- **管理者の指示に従い、アンチウィルスソフトウェアの駆除機能によってウィルスの駆除を試みる。**
- **駆除が成功したと思われる場合には、当該パソコンと接触のある機器（例えば、 USB メモリ、外付けハードディスク、研究室内のパソコンなど。）全てに対して、管理者の指示に従い、同様の処置を施す。**
- **以上でウィルス駆除ができない場合は、管理者の指示に従って対策方法を検索する。**

アンチウィルスソフトウェアによってウィルス駆除ができない場合は、システムそのものをクリーンインストールする方が簡単な場合があります。また、最近の流行のワンクリックウェア（「アダルトサイトの利用料を支払え」といった内容のウィンドウが定期的にデスクトップ上に表示される）については、アンチウィルスソフトウェアで駆除できない場合が多いようですので、管理者に相談して下さい.

（5）校外へパソコンを持ち出す場合

学会などでの学外発表、各種コンテスト、行事等で校外へパソコンを持ち出す場合の注意事項を示します。（学校が保有・管理するパソコンだけでなく、学校内で使用したパソコンを校外へ持ち出す場合についても以下の事項を守るようにして下さい。）

校外へパソコンを持ち出す場合の注意事項

- **機密性3情報[注6]を保存したパソコンは、校外へ持ち出さないこと。(機密性3情報を保存したパソコンに限らず、"学校のパソコンを校外に持ち出す場合は事前に管理者の許可が必要である"といった規則を定めている学校もあります。その場合には所定の手続きをとって下さい。)**
- **「(2)校内でパソコンを利用する場合」の注意事項を校外においても遵守し、禁止事項は行わないこと。ただし、個人や学外団体保有のパソコンを、保有者の活動目的のために使用することは勿論かまいません。**
- **持ち出した後に、校内に戻す場合には、ウィルスチェックを行うこと。**

以上の通りですが、著作権侵害を引き起こす可能性がある状態での P2P ファイル共有ソフトウェアの利用については校内・外を問わず禁止します。また、盗難、紛失、情報漏えいなどのリスクがあるため、「機密性3情報」[注6]を保存したパソコンの持ち出しは禁止しますが、どうしても持ち出しが必要な場合には情報セキュリティ副責任者に相談して下さい。

「機密性3情報」[注6]を保存したディスクや USB メモリも同様です。

[注6]第1章(4)情報セキュリティ対策の解説記事、特に[解説4]機密性、完全性、可用性とは?を参照して下さい。

(6)校外から情報システムを利用する場合

自宅等の校外から情報システムを利用する際に、利用できる接続形態と、使用するパソコンについての注意事項を示します。

利用できる接続形態

利用できる接続形態の種類として、「VPN」と「学認(※)」が挙げられ、以下の様な特徴があります。

(※)「学認」は、近日導入予定です。

- **VPN(Virtual Private Network)**
  インターネットを利用する際に暗号化や認証等の技術を適用してセキュリティを確保したネットワークを指します。VPN には、SSL-VPN(SSL(Secure Socket Layer)プロトコルを使用し、ブラウザを介した通信上のデータを暗号化する技術で、指定されたブラウザがあれば、他のソフトウェア等を用意する必要はありません。)と IPsec-VPN(IPsec(Security Architecture for Internet Protocol)を使用し、アプリケーションに依らず通信上のデータを暗号化する技術で、専用の VPN クライアントソフトウェアをパソコンにインストールする必要があります。)の 2 種類があり、各校のサービスによって、使用する種類が異なります。

- **学認**
  全国の大学等と NII(国立情報学研究所)が連携して構築・運用する「学術認証フェデレーション」の愛称で、Web アプリケーションへのシングル・サイン・オン(1 つの ID・パスワードであらゆるシステムが利用可能であること)技術を、組織を越えて活用する分散型認証基盤です。認証の連携により、学内でのシングル・サイン・オンを実現可能とし、NII が提供するデータベースジャーナル「CiNii」をはじめとした学外のサービスにおいても、1 つのパスワードを利用し，かつ ID・パスワードの再入力を行わずに利用できる環境を実現することができます。

使用するパソコンについての注意事項

- **利用しているコンピュータの OS の「セキュリティアップデート」(Windows Update など)を定期的に実行し、セキュリティホールを狙った攻撃(ウィルス感染や侵入)を防止すること。**
- **アンチウィルスソフトウェアを導入すること。**
- **アンチウィルスソフトウェアのウィルス定義ファイルを常に最新の状態に保つこと。**
- **アンチウィルスソフトウェアによって、定期的にパソコン内のファイルや USB メモリのファイルをチェックすること。**
- **出所の定かでないソフトウェアをインストール、使用しないこと。**
- **P2P ファイル共有ソフトウェアをインストール、使用しないこと。**
- **インターネットカフェ等、不特定多数の人間が使用するパソコンは使用しないこと。**

4. 情報セキュリティインシデントを見つけた場合

下記のような場合には学校の教職員または管理者に連絡して指示を受けて下さい。

教職員または管理者に状況を連絡すべき場合

- **学校のサーバ上に、著作権を侵害しているおそれのあるコンテンツや、機密情報（秘密にしなければならない情報のことで、情報セキュリティ対策の用語では、「機密性3又は機密性2の情報[注7]」と呼びます。）が公開されていることを発見した場合。**
- **学校のサーバ上にある重要な情報（間違いのない状態でいつでも利用できるようにしておかなければならない情報のことで、情報セキュリティ対策の用語では、「完全性2かつ可用性2である情報[注7]」と呼びます。）に誤りや欠落を見つけた場合。**
- **インターネット上などで、学校に関する機密情報（上記の通り。本校学生や教職員の個人情報を含みます。）が公開されている、又は学校が権利を有するコンテンツが無断で使用されていることを発見した場合。**
- **自分が管理するユーザ ID やパスワードが漏えいした、またはその可能性がある場合。**
- **P2P ファイル共有ソフトウェアを利用しているパソコン、あるいは学生や教職員を知っている場合。**

［注7］第1章（4）情報セキュリティ対策の解説記事、特に**［解説4］機密性、完全性、可用性とは？**を参照して下さい。

前述のような場合は、一般に**情報セキュリティインシデント**と呼ばれる事象の一種で、学校の情報セキュリティの確保を困難にしてしまう状況です。

［解説7］情報セキュリティインシデントとは？

情報セキュリティの確保を困難にする原因の発生及び発生の恐れを言います。つぎの3種類があります。

■物理的インシデント

地震や落雷などの自然災害、建物の倒壊や火災、情報システムや文書の盗難など、情報システムの機能不全を招く物理的状況。

■システムインシデント

情報システムの稼働を妨害する行為、データ改ざん・消失・漏えい・暴露を引き起こす行為、ネットワーク及びコンピュータ資源を浪費する行為などが行われている状況。

■コンテンツインシデント

法令又は公序良俗に違反する情報を発信する行為、及びその恐れがある状況。

5. 電子メール

(1)電子メールの利用

電子メールは、電話と違い相手が不在の際でも情報を伝達することが可能です。画像やワープロ文書なども送信可能で便利なツールですが、以下の注意事項を守る必要があります。

電子メールについての注意事項

- **就職等の重要な連絡については、電話などで確認をとるなど慎重な利用を心がけること。(送信後直ちに届くとは限りません。送信途中のサーバやネットワークの状態によっては時間がかかることも、届かないこともあります。)**
- **送信途中の第三者によってメールの内容を盗聴される可能性がある、システム上のトラブルを解決するためにサーバ管理者が検査する場合がある、最終的には裁判などの証拠とされる場合がある、などの可能性を承知した上で送信内容及びそれに適した送信方法を考えること。**
- **機密情報を送信する場合には暗号化などの対策を実施すること。(パスワードや個人情報等のデータの送付はできるだけ避けて下さい。)また、宛先が間違っていないかどうかをよく確認すること。**
- **身に覚えがない電子メールは開かないこと。迷惑メールは無視して即削除すること。**
- **アダルトサービスなどの「利用料金を払わないと法的手段に訴える」等のメールには一切返信しないこと。(このようなメールは詐欺を目的として送られている場合がほとんどです。身に覚えがある場合でも、でたらめに送付された可能性があります。このようなメールに返信してしまった場合には学校や最寄りの消費生活センター等に相談して下さい。)**

(2)電子メール利用の一般的マナー

電子メールを利用する場合に守るべき一般的マナーを示します。

電子メールを利用する場合のマナー

- **電子メールのサイズ(添付データを含む)に気をつけること。(相手によって異なりますが、校外に対して500 kB～1MB を超える電子メールは送信しないようにして下さい。)**

- 添付ファイルは極力使用しないようにすること。（受信した人にウィルス感染させる危険性があります。）
- 「不幸（幸福）の手紙」、「“セキュリティ上の問題点をできるだけ多くの知人に知らせるように”」といった善意を装った不特定多数への配布を目的としたチェーンメールを他人に転送しないこと。
- ㈱や①のような機種依存文字を使わないこと。（相手側で読めないことがあります。）
- HTML 形式のメールを送信しないこと。（ Microsoft 社のメールソフトである Outlook は標準で HTML 形式のメールを送信してしまいます。セキュリティ上の問題もありますので、必ず解除しましょう。）
- メーリングリストではサイズの大きい添付ファイルをつけないこと。自動返信の機能を用いないこと。

（3）電子メール利用の際の禁止事項

電子メールを利用する際の禁止事項を以下に示します。

電子メールを利用する際の禁止事項

- 電子メールアカウントを他人に利用させること。
- 本人以外のメールアカウント（クラブや学生会等に対するもののことです。）を付与あるいは利用許可された場合に、そのアカウントを関係者以外に利用させること。
- 学校の業務に必要でないメーリングリスト等へ登録すること。
- ウィルス対策ソフトウェアのインストールが確認できないコンピュータ上で電子メールを送受信すること。
- 迷惑メールの送信を行うこと。
- 「自己解凍形式（.exe 等）」の添付ファイルを使うこと。
- セキュリティ上の安全性が確認できないマクロを含んだファイルを送信すること。

6. ウェブ

（1）ウェブブラウザ（WWW サービス）の利用

ウェブブラウザによる WWW サービスは、多くの情報を我々にもたらしてくれますが、やはり色々な危険性が潜んでいます。次の注意事項を守って下さい。

ウェブブラウザを利用する際の注意事項

- **ブラウザのセキュリティ対策に気を配ること。ブラウザには修正プログラムを適用し、可能な限り最新の状態にすること。**
- **パスワード等の保存は慎重に行うこと。（共用コンピュータ上での保存は避けて下さい。）**
- **作成元が明確でないプラグインを導入しないこと。**

（2）ウェブサービス利用の際の禁止事項

ウェブサービスを利用する際の禁止事項を示しておきます。

ウェブサービスを利用する際の禁止事項

- **学校の業務に必要のないサービスを利用すること。（不正サイトへの接続は厳に慎しんで下さい。また、懸賞やゲームの無料サイトへの接続もしないで下さい。）**
- **機密情報 [注8]を校外の掲示板、 SNS サイト、ブログへ書き込んだり、ツイッターでの発言やウェブメールの中で漏えいさせてしまうこと。（特に成績や住所等を公開してしまわないように注意して下さい。）**
- **誹謗中傷や公序良俗に反する内容、反社会的な内容を書き込むこと。（発言・書き込みには責任が伴うことを理解して下さい。）**
- **迷惑メールなどの電子メールで送付されてきた URL をクリックすること。（信頼できないサイトへは接続しないようにして下さい。）**
- **著作権によって保護されているデータの閲覧、ダウンロードを行うこと。**
- **アンチウィルスソフトウェアによって、コンピュータウィルスに感染しているデータかどうかを確認せずに、ダウンロードしたデータやプログラムを開くこと。**

［注8］**機密情報**とは、機密性3又は機密性2の情報のことです。詳しくは、第1章（4）情報セキュリティ対策の解説記事、特に**［解説4］機密性、完全性、可用性とは？**を参照して下さい。

（3）ホームページの見分け方

危険なホームページの見分け方を説明しておきます。

危険なホームページの見分け方

◆ **アダルト情報を含むホームページ**

巧みな方法によって、数回のクリックで「利用契約が成立しました。情報利用料が発生します」という画面を表示する場合があります。このような方法で金銭をだまし取ることをワンクリック（場合によってはツークリック）詐欺と呼びます。信頼できないサイトを利用しないのが一番の対策ですが、仮に高額な情報利用料を請求された場合でも、電話をかけたり電子メールで連絡を取ったりしないようにして下さい。電話番号やメールアドレスが相手側に知られてしまった場合は、学校や消費生活センター等に相談して下さい。

◆ **無料を装って個人情報を収集するホームページ**

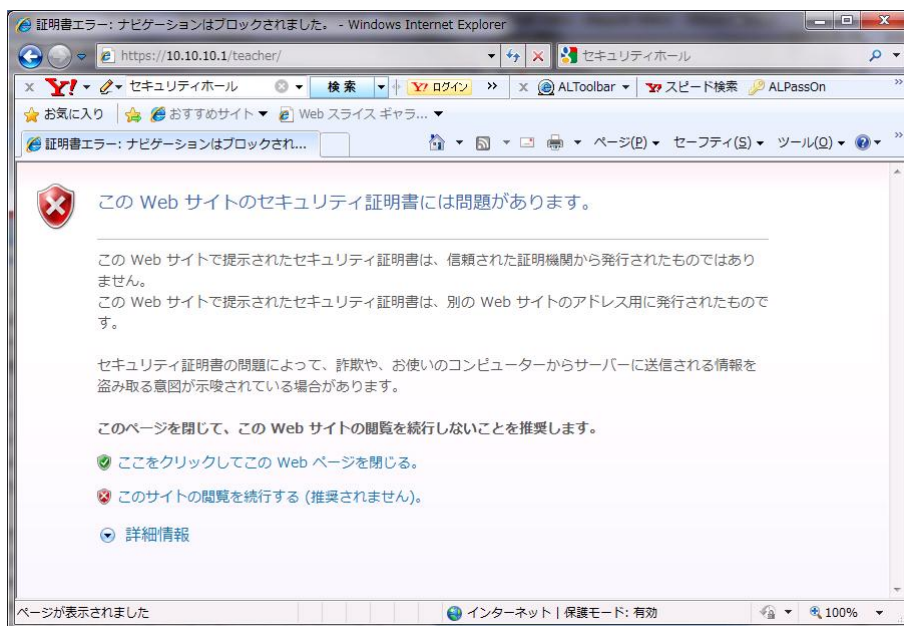
無料のゲームサイト、無料の着信メロディなどを提供するサイトには、メールアドレス等を登録させるところが多くあります。登録後に迷惑メールが激増した、広告メールが増えて困っている、ということをよく聞きます。「うまい話には裏がある」、ということを常に考えて行動して下さい。

◆ **有名メーカーなどのホームページ**

一般的によく知られている有名メーカーのホームページは信頼できます。ただし、有名銀行などを装った偽のホームページを作成し、口座番号や暗証番号等を盗み取るサイトもあります（このような詐欺をフィッシング詐欺と呼びます。）ので、「釣られない」ようにして下さい。ホームページのアドレス（ URL あるいは URI）の「http://」の直後に、見慣れない数値（ IP アドレスと言います。たとえば、http://201.12.31.11/hogebank.co.jp など）が現れるサイトには十分に注意する必要があります。

◆ **サイト証明（SSL）の確認**

住所などの個人情報の入力の際にはサイト証明を確認することが重要ですが、下記のように偽のサイト証明である場合も考えられますから十分注意して下さい。

オンラインショッピングなどの決済（クレジットカード情報の入力）や住所などの個人情報の入力の際に URL（インターネット上のホームページを示すアドレス）が http://～ではなく、 https://～となる場合があります。「 https://～」は通信そのものが暗号化されて安全な通信が行えることを示していると同時に、相手の WWW サーバが目的とするサーバとして正しいかどうか（「なりすまし」や「偽装サーバ」でないか）を第三者が証明をするものです。ただし、誰がそれを証明しているかが問題です。悪意を持った者が自分でそ

信頼できない信頼できない第三者の証明書の例

れを証明しようとする場合や、別の似た名前で登録をしている場合があります。

たとえば、「 ○○銀行」へ接続するつもりの人を、悪意を持った偽のサーバへ誘導する場合を考えてみましょう。悪意を持った偽のサーバは、公式に「 ○○銀行」としてきちんとした第三者の証明を受けられません。（例えばベリサイン社などは信頼できる第三者として知られています。）この場合は、第三者に偽の証明書を発行してもらうか、似た別の名前を名乗ることをします。（例えば、「○○銀協会」や、英語で ○○ Inc. などです。）偽の証明書の場合には図1のような画面が現れます。このような警告が現れる場合、接続先の URL がいつも利用している正しいサイトかどうか確認を行い、確認ができない場合は接続しないようにして下さい[注9]。また、証明書が提示されている場合は、そこに書かれた詳細情報を表示し、会社名などが正しいかどうかを確認しましょう。

[注9]一部情報システムでも同様な警告が現れますが、URL が正しい場合は接続して頂いて問題ありません。

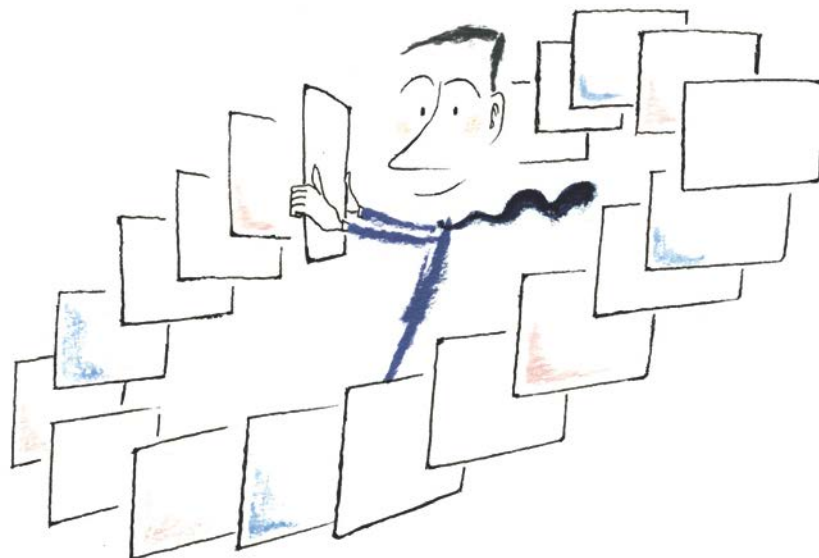
（4）電子掲示板やブログ、ツィッター等を利用する際の注意

電子掲示板での意見交換、会員制 SNS サイトなどで利用されているブログ等では自分の思いがうまく伝わらない場合があります。軽い冗談のつもりが、相手を怒らせてしまうこともありますので、発言には細心の注意が必要です。

会員制 SNS サイトでは、そのほとんどで日記や日々の出来事、自分の意見などをブログによって公開できるようになっています。しかし、プロフィールから実名や所属する学校名（企業名）が特定（あるいは推測）されることがあります。ブログ中で「犯罪 」や「反社会的活動」の自慢を行い、「解雇（地方公務員）」、「内定取り消し（大学生）」となったケースがあります。また、電子掲示板やブログでの発言で、悪ふざけが悪ふざけで済まなくなったケースもあります。たとえば、掲示板において、名指しで特定の人の批判を行うことで「名誉毀損」の罪で逮捕されたり、本気でなくとも「小学校を爆破する」、「○○駅で秋葉原通り魔殺人事件を再現したい」などという犯罪予告を行って「威力業務妨害」などで逮捕されたケースがあります。

以上のように、SNS や掲示板は私的な「交換日記」ではありません。「不特定多数のユーザから常に見られている」、「自分も社会の一員である」という意識を常に持って利用する必要があります。

SNS、掲示板における一般的注意事項

- **いたずら書きや喧嘩腰での議論をしないこと。（これは電子掲示板を利用する際に、必ず守らなければならないマナーです。なお、書きこみに使われたコンピュータのアドレス情報も同時に記録されている電子掲示板もあり、学校へ苦情が寄せられることがあります。）**
- **発言には責任を持つこと。（個人として書き込む場合でも、組織内のネットワークから書き込むと、その組織からの書き込みとして組織全体の意見と受け取られる危険性があります。発言は責任を持って行って下さい。）**
- **他人の意見は寛大に受け取ること。（もし、他人の無責任ととれる発言があっても、本人にはそのつもりがないかもしれません。電子掲示板上での言い争いは、読む人や電子掲示板の管理者にと って迷惑となります。反論がある場合にも、少し時間を置いて、よく一度考え直してみることが大切です。感情的になって直ちに返信することは避けて下さい。）**
- **犯罪自慢や反社会的発言は絶対に行わないこと。（たとえ冗談であっても犯罪や反社会的活動を自慢することは厳禁です。事実でなくとも社会的に影響があったという理由で解雇や処分、内定取り消しなどが行われる場合があります。）**

7. ウェブを公開する場合

(1)ウェブ公開についての全般的注意

インターネット普及の立役者と言えるのが、WWW(World Wide Web)による情報公開・共有です。WWWサーバによる情報発信は現在のインターネットでは必要不可欠の行為であり、本校でも教職員はもちろん、学生会と一部のクラブについて、WWW サービスによる情報発信を認めています。一方で、各種の権利侵害を伴うようなウェブコンテンツの公開や掲示板等の開設は、そのトラブル対応により業務効率を低下させ、さらに学校の社会的信用を失わせる結果となります。ここでは、このようなリスクを軽減し、情報資産を保護した上で、各種コンテンツや情報を正確・安全に公開するために必要な事項を説明します。

WWW サーバを用いて各種情報を公開する際には、各種法令を遵守することはもちろんのこと、契約している ISP(インターネット接続サービスを提供する業者)の利用規約や学校の規則を守らなければなりません。公序良俗に反する行為や、反社会的な行為を行ってはなりません。

ウェブ公開における全般的注意事項

- **学校の業務目的以外のウェブ公開は行わないこと。**
- **営利を目的とした利用を行わないこと。**
- **通信の秘密を侵害しないこと。(通信の盗聴は特別な場合を除き行ってはなりません。)**
- **過度な負荷をかけるなど、ネットワークの運用に支障を及ぼすような利用をしないこと。**
- **ネットワーク及び接続するコンピュータに対する不正行為等が発生しないように最善の努力を払うこと。**

ウェブを用いた情報公開には大きなメリットがある反面、様々な危険やリスクを伴うことを理解しておかなくてはなりません。また、情報発信者の責任として、その意義と危険性についての十分な認識が求められます。

ウェブ公開において不正行為を防止するための注意事項

- **公開を行うデータの安全性(コンピュータウィルスの有無)を確認すること。**
- **圧縮形式のデータを提供する場合、自己解凍形式のデータを提供しないこと。**
- **電子署名されていない実行モジュール(Java アプレット、ActiveX コントロールなど)を使用しないこと。**

- **電子署名は可能な限り第三者が保証したものを利用すること。**
- **学校のウェブコンテンツを参照する際に、ブラウザのセキュリティ設定を変更するような要求を行わないこと。**
- **学校のウェブコンテンツを参照するために、安全性が保証されないソフトウェアのインストールを要求しないこと。**
- **セキュリティ上の安全性が確認できないマクロを含んだファイルを提供しないこと。**

（2）その他、注意すべき事項

■著作権等の知的財産権の遵守

他人が保有する知的財産権を侵害してはなりません。自分の作ったコンテンツ以外は原則として許諾なしに掲載してはいけません。ウェブに公開することを著作権者が許諾する「公衆送信権（送信可能化権）」は、通常の複製を許諾する「複製権」とは別の権利となっています。したがって、複製（コピー）を許可された場合でも、ウェブ上に公開する行為が認められない場合があります。ただし、参考文献などの形で出典を適切に明示した上で、その文献の一部分を「引用」することは認められます。（→第９章（２）参照）

■肖像権への配慮

人は人格権的な権利として、肖像権を有すると考えられています。他人の顔が写っている写真等を掲載する際には、「肖像権」に十分注意して下さい。一般的には、本人の許諾なしに写真を掲載するべきではありません。（→第９章（４）参照）

■他人に迷惑をかけるような情報発信の禁止

ウェブ上で情報発信する際は、他人に迷惑をかけるような情報を発信してはなりません。他人に迷惑をかけるような情報としては、差別、名誉毀損、人を誹謗中傷する内容のもの、個人情報や他者のプライバシーを侵害するような情報、ハラスメントなどがあります。（→第９章（５）参照）

■研究成果や研究途中の情報など守秘義務に違反する情報公開

研究成果や研究途中の情報を掲載する際には、公開に問題がないか十分検討して下さい。特に、実習・インターンシップ先で得た情報については、守秘義務に違反しないように十分注意して下さい。

■企業名やロゴなどの扱い

学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に相手側と協議して下さい。
（→第９章（３）参照）

■顔写真の掲載

自身の肖像写真を掲載する場合にも、顔を露出する際のリスクを十分に考慮して下さい。（→第９章（４）参照）

■公序良俗に反する情報

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはなりません。

■デジタルアーカイブを行う場合

古典資料などのデータをウェブで公開する際には、事前に各種権利処理が済んでいるかをきちんと確認して下さい。

■リンク情報

リンクの設定そのものは相手の許諾を得ることなしに自由に行えるとされています。しかし、トップページ以外の階層へ直接リンクを張ることが許されない場合があります。

■政治・宗教などの情報

個人ページや各研究室サーバからの政治や宗教などに関する情報の発信を禁止します。

■隠しディレクトリに関する注意

公開すべきでない情報は、たとえ隠しディレクトリであっても置かないようにして下さい。

■公開掲示板（BBS）等の開設の禁止

許可なく研究室サーバや個人のサーバで公開掲示板（ BBS）等を開設することを禁止します。

■学校の社会的信用を失墜させるような情報の発信の禁止、法令に反するあるいは損害賠償等の民事責任を発生させるような情報の発信の禁止

学校の社会的信用を失墜させるような情報発信、法令によって処罰の対象とされるような情報発信、及び損害賠償等の民事責任を発生させるような情報発信を禁止します。（あやふやな情報発信によって生産・販売者に風評被害を与えた場合、損害賠償請求に発展することがありますから、十分注意して下さい。）なお、法律や学校の情報セキュリティ実施規程等に違反する行為が認められた場合には、運用者の承諾なしにウェブコンテンツの削除やウェブサーバの隔離等の措置をとることがあります。

8. パソコンの保全・管理対策

パソコンの保全・管理における注意事項

- ◆ ID／パスワードの管理を徹底すること。
- ◆ 必要に応じて盗難防止策と BIOS[注10]レベルでのパスワード設定を行なうこと。（重要なデータが入っているパソコンは、持ち出しができないように専用のチェーン等でロックするなどの対策をとって下さい。なお、 BIOS レベルでのパスワードを設定しておくことで、パスワードを入力しないとパソコンの起動さえ不可能にすることができます。）
- ◆ 資産管理を徹底させること。（資産管理が不十分だと、最悪の場合、盗難に遭ったことさえわからなくなります。パソコンの備品番号、利用者、設置場所、利用内容など、必要な情報を管理して下さい。）
- ◆ 廃棄時はディスク内容を消去すること。（古くなったパソコンを処分する場合、内部には重要なデータが残されているかもしれません。廃棄する際はディスクを物理的に破壊する、あるいは完全にデータを消去する、又は別のデータで上書きする等の対策をとってください。通常の操作でファイルを消しただけでは、専用のソフトウェアを使用することでファイルを復元できます。データが完全に消えるわけではありません。）
- ◆ パソコンの修理を業者に依頼する場合は、機密情報、個人情報の漏えい防止策を講じた上で行うこと。判断が難しい場合は、情報セキュリティ推進委員長あるいは副委員長に相談の上修理を依頼すること。

［注10］BIOS とは、パソコンが動作するために必要な基本的ソフトウェア（Basic Input Output System）で、オペレーティングシステムが起動する前に読み込まれます。

9. 付録

(1)電子決済・インターネットバンキング・オンラインショッピング等

最近、インターネット上での通信販売を利用する人も増えてきました。利用代金の支払いを着払い・銀行振込にする方法もありますが、現金を使用せずにクレジットカードなどを活用して支払いを行っている人も増えています。また、インターネット上で預金や振り込みが可能なインターネットバンキングを利用する人もいるでしょう。ここでは、オンラインショッピングと**電子決済**、**インターネットバンキング**等について説明します。もちろん学校の情報資産を私的な目的に利用することは禁じられていますから、ここでの注意事項は自宅や学外において自分のパソコンで利用する場合に関するものです。

[解説8]電子決済とは？

電子商取引の購入代金、使用料金などの決済をネットワークや IC カードを利用して行うことを電子決済と言いますが、それには次のようなものがあります。

- **電子マネー**
  電子的なデータに貨幣価値を持たせたもので、IC カード型とネットワーク型に分類されます。ICカード型は実店舗での利用を目的としたものです。ネットワーク型はインターネット仮想店舗での決済のため、パソコン上に組込まれた電子情報(貨幣価値)により決済する方法です。
- **クレジットカード決済**
  現在最も代表的な方式です。クレジットカードの番号を仮想店舗のホームページから入力、送信して、決済する方式です。
- **インターネットバンキング**
  インターネット上から残高照会や振込手続きを行うことにより銀行口座での決済をする方法です。
- **電子小切手**
  小切手帳の機能を電子化し、端末の画面でデジタル署名を行う決済方式です。

オンラインショッピングの利用者にとって恐いのは、送金したのに商品が送られて来ない、買ってもいない商品の代金が請求される、などです。信頼できるショップを選び、決済方法やセキュリティ対策を見極めることが重要です。注意事項を示します。

オンラインショッピングにおける注意事項

- **ショップの信頼性を確認すること。(ショップのホームページでフリーメールではない電子メールアドレスが公開されているか、一般加入電話のように契約者が特定できる電話番号が公開されているかを確認して下さい。)**

- **決済方法を確認すること。（前払い方式の決済の場合で、ショップに信頼性がない場合は商品が送られてこない危険性があります。高額な商品は避ける、代金引換方式のショップを利用するなどを検討して下さい。）**
- **セキュリティ対策が実施されているか確認すること。（クレジットカード番号、個人の情報などを暗号化して送る仕組みが提供されているかを確認して下さい。少なくともクレジットカード決済の場合は SSL（Secure Sockets Layer）などによる暗号化の対策が実施されているショップを選んで下さい。ホームページのアドレス（ URL）の先頭が http ではなく https になっていれば SSL による暗号化対策が実施されています。）**
- **クレジットカード利用状況を確認すること。（自分が利用しているクレジットカードの利用状況を常に把握し、自分の知らないところで不明な引落し等が発生していないか日頃からチェックして下さい。）**

個人経営の商店だから、セキュリティも弱いとは限りません。ショッピングモールと呼ばれる仮想商店街に出店することで、ショッピングモールが提供しているセキュリティ対策機能を利用し、信頼性を高めている例もあります。経営の規模では無く、ホームページのアドレスやホームページの内容により信頼性を確認するとよいでしょう。

（2）著作権の侵害

制作者（著作者）の利益を保護するために著作権法が制定されています。**著作権**と一言でいってもいろいろな権利の総称で、実際には以下のような権利が含まれています。他人の著作物を利用する場合には著作者の許可が必要です。

［解説9］著作権

著作権を保有した者が持つ権利には次のようなものがあります。

・複製権（著作物を複製する権利）
・公衆送信権
・展示権
・頒布権
・貸与権
・二次的著作物の利用に関する権利
・上演権／演奏権
・口述権
・上映権
・譲渡権
・翻訳権／翻案権

［解説10］著作権の許可が不要な例

■ 私的利用のための、個人的、家庭内など限られた範囲での使用。
■ プログラムのバックアップのための複製や自ら使用するための改変。
（ただし、コピー防止機能を解除してのコピーは違法です。）
■ 参考文献を明示した上での部分的な引用。
■ 教育機関による、学校教育の目的上必要な範囲の使用。（授業教材としてのコピーなどを指す。ただしソフトウェアのコピーは除かれます。）

著作権侵害を行った場合のペナルティ

『 著作権で保護されたデータを提供(アップロード)した場合 』

- **懲役10年以下あるいは1000万円以下の罰金**
- **民事訴訟による損害賠償金・・・購入代金の3倍 ×想定コピー数**

『 著作権で保護されたデータを入手(ダウンロード)した場合 』

- **懲役2年以下あるいは200万円以下の罰金、またはその両方**
- **民事訴訟による損害賠償金・・・購入代金の3倍 ×想定コピー数**

「1000万円以下の罰金」は、万引きなどの窃盗による刑罰(懲役10年以下、50万円以下の罰金)よりも重いことに注意して下さい。なお、「民事訴訟による損害賠償金は、億単位の額になる」判例があります。

P2P ファイル共有ソフトウェアによっては、そのしくみからダウンロード、アップロードが不可分なものがあります。著作権保護されたデータをダウンロードしているだけのつもりが、気がつかないうちに他人にデータ提供を行っている場合があり、「アップロード」と見なされる可能性があります。技術者は知的財産を産みだし、守る立場です。その技術者(技術者の卵=学生)が著作権侵害を行うことは自殺行為でもあり、学校や高専全体の信用を失墜させてしまいます。

(事例)2009年 11 月 秋田県に住む主婦(38 歳)が韓国ドラマの動画データを P2P ファイル共有ソフトウェアで入手・そのまま公開・・・懲役 1 年6月、執行猶予3年の刑が確定

(3)商標の使用

「**商標**」は主に商売と密接な関係があり、商品名、サービス名、商品の形状、ロゴやマークなどが対象となります。他人の商標を、自分の商品やサービスに使用すると**商標権の侵害**となります。同じでなくても混同されるような名称を使うのは不正競争防止法違反となる場合がありますので注意して下さい。

[解説11]商標と商標侵害の例

商標

■ 商品名、サービス名、商品の形状、ロゴやマークなどを商標といいます。商標法に基づき登録を行なった商標を登録商標と言い、商標権が発生します。

商標権侵害とならない場合

- ■ 商標は指定商品・指定サービス内でのみ有効であるため、同じであっても全く種類の異なる商品やサービスに利用する場合は侵害になりません。（例：チョコレート菓子の「小枝」と芸名の「小枝」）
- ■ 自分の商品などの説明のために、他者の商標を普通に使用する場合は侵害となりません。

商標権侵害とはならないが別の法律で制限されている場合

- ■ 他人の商標と同じではないが似ている名前で同様の商品、サービスなどを提供すると、商標権侵害とはならなくても、「不正競争防止法」違反となる場合がありますので注意が必要です

（4）肖像権/プライバシーの侵害

自分で撮った写真をホームページに掲載する場合、著作権は自分にあるので一般的には問題ありません。ただし、他の人物が写っている写真などについては**肖像権やプライバシー**に気を付ける必要があります。プライバシーの権利は個人情報（個人を特定できる情報）をみだりに公開されないという権利です。肖像権はプライバシー権のひとつとなります。

［解説12］プライバシー（肖像権）の侵害の例

プライバシー（肖像権）の侵害となる場合

- ■ 本人への断わりなく、本人の情報を公開するとプライバシーの侵害となります。
- ■ 本人への断わりなく、本人の写真を公開すると肖像権の侵害となります。

侵害とならない場合

- ■ 本人の許可があればもちろん侵害となりません。
- ■ 写真の場合でも本人と特定できない場合は肖像権侵害とはなりません。

有名人の場合は肖像自体に経済的な価値がありパブリシティ権（財産的に利用する権利）が認められます。個人が有名人の写真を許可なく使うと肖像権の侵害となり、自分で撮影した写真でない場合は著作権の侵害にもなります。さらに、有名人の写真を使うことで結果的に利益を生み出すような場合はこのパブリシティの権利も侵害することになります。

（5）名誉毀損/偽計業務妨害/電子計算機損壊等業務妨害/不正指令電磁的記録作成罪

電子掲示板やホームページに記載された（掲載された）情報は公開されたことになります。このような場で、他者の社会的評価を低下させるような表現を行なうと、「名誉毀損」となる場合があります。「名誉毀損」には刑事罰が適用されます。また、虚偽の風説などを流して業務を妨害する行為、威力を用いて業務を妨害する行為は「偽計業務妨害」又は「威力業務妨害」と呼ばれます。さらに、コンピュータに虚偽のデータや不正な実行を行わせて業務を妨害する行為は「電子計算機損壊等業務妨害」と言います。たとえば、知らないうちにコンピュータウィルスがある企業のサーバを攻撃して機能をマヒさせてしまった場合、威力業務妨害ないし電子計算機損壊等業務妨害に相当します。また、コンピュータウィルスを作成、配布する行

為は不正指令電磁的記録作成罪に相当します。

名誉毀損、偽計業務妨害、電子計算機損壊等業務妨害に関する法律

◆　**名誉毀損【民法710、723条】**

品性、徳行、名声、信用その他の人格的価値について社会から受ける客観的評価(社会的評価)を低下させる行為の禁止。損害賠償責任が肯定されています。

◆　**信用および業務に対する罪【刑法第 168、233、234 条】**

虚偽の風説を流し、または偽計を用いて人の業務を妨害すること(偽計業務妨害罪)。または威力を用いて人の業務を妨害すること(威力業務妨害罪)。他人のコンピュータやその電磁的記録の損壊、不正な指令などで業務を妨害する行為(電子計算機損壊等業務妨害罪)については、5年以下の懲役または100万以下の罰金、コンピュータウィルスを作成、または提供する行為（不正指令電磁的記録作成罪)については、3年以下の懲役または50万円以下の罰金に処せられます。

[解説13]名誉毀損について

公共の利益とみなされる場合

■　摘示(要点をかいつまんで示したり、隠していることをあばいたりすること。)された事実が公共の利害に関するものであり、かつ行為の目的が専ら公益を図ることにあって、摘示された事実が真実であることの立証がある場合は名誉毀損になりません。
(例)
あるメーカーの機械が粗悪品のために怪我をする可能性があるので、電子掲示板にメーカー名や製品名を挙げて欠点を書き込んだ。

単なる誹謗中傷の場合

■　バカ、アホ呼ばわりのような誹謗中傷行為は名誉毀損であり、モラルの点からもやってはいけません。場合によっては、法的責任を問われて重大な問題に発展することがあります。

相手が訴えた場合

■　名誉毀損罪は親告罪のため相手が告訴しなければ罪にはなりませんが、告訴された場合「逮捕」される可能性もあります。

（6）わいせつな文書や画像の発信

わいせつか芸術かの判断は難しいのですが、ホームページなどに掲載した情報が「わいせつ」であると判断されると次のような法律によって処罰されます。

わいせつな情報発信に対する罰則

◆ **【刑法（明治 40 年法律第 45 号） 第 175 条】**

わいせつな文書、図画その他の物を頒布し、販売し、又は公然と陳列した者は、 2 年以下の懲役又は 250 万円以下の罰金若しくは科料に処する。販売の目的でこれらの物を所持した者も、同様とする。

◆ **【児童買春・児童ポルノに係る行為等の処罰及び児童の保護に関する法律（平成 11 年法律第 52 号）第 7 条第 4 項】**

児童ポルノを不特定若しくは多数の者に提供し、又は公然と陳列した者は、5 年以下の懲役若しくは 500 万円以下の罰金に処し、又はこれを併科する。電気通信回線を通じて第二条第三項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録その他の記録を不特定又は多数の者に提供した者も、同様とする。

（7）不正アクセス禁止法

2000 年 2 月 13 日に「不正アクセス行為の禁止等に関する法律」いわゆる不正アクセス禁止法が施行されました。その概要はつぎの通りです。

不正アクセス禁止法の概要

次の行為が禁止されていて、何の実害を与えなくても処罰の対象になります。

『 不正アクセス行為 』

- **アクセスが制限されたコンピュータに対し、他人のユーザID／パスワードを使ってログイン（コンピュータが使える状態に）すること。**
- **アクセスが制限されたコンピュータに対し、セキュリティホールをついて侵入し、コンピュータが使える状態にすること。**

『 不正アクセス行為を助長する行為 』

- **偽サイト（フィッシングサイト）を作成して閲覧可能にすること。**
- **偽サイト（フィッシングサイト）に誘導するメールを送信すること。**

- **他人のユーザID／パスワードを当該コンピュータの管理者、当該ユーザID／パスワードの利用者以外に提供すること。**

ただし、次のような場合は不正アクセス行為に該当しないものと考えられています。
・パソコン初心者に頼まれて接続操作を行なってあげた。
・コンピュータの管理者自ら、もしくは管理者の承諾を得た者が行なった。

（8）電波法および盗聴

ネットワーク上の情報の盗聴は禁止されています。また、盗聴した内容を第三者に漏らす行為についても電波法、電気通信事業法違反となり罰せられます。

電波法、電気通信事業法による規制

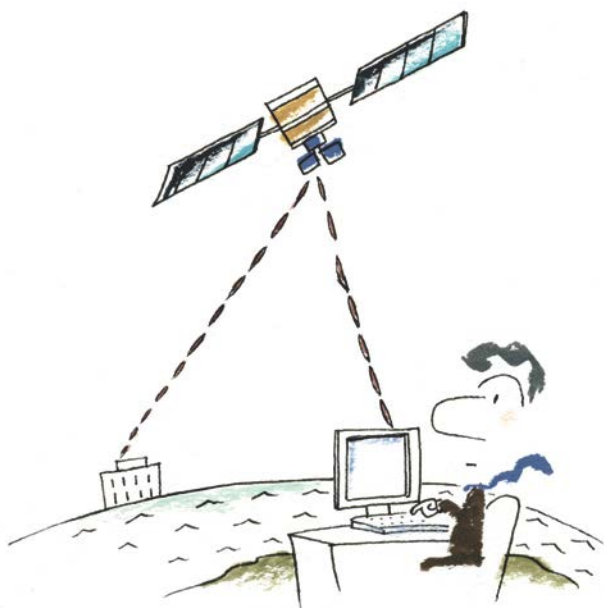
◆ **有線通信における秘密の保護【有線電気通信法第9条】**

電話や FAX、インターネットなど有線でつながれた方法で得た秘密や情報は他人に話してはならない。（違反した者は 1 年以下の懲役または20万円以下の罰金に処せられます。）

◆ **無線通信における秘密の保護【電波法第 59 条】**

特定の相手に対して行われる無線通信を傍受してその存在もしくは内容を漏らし、盗用してはならない。（違反した者は 1 年以下の懲役または20万円以下の罰金に処せられます。）

◆ **電気通信事業者の守秘義務【電気通信事業法第4条】**

電気通信事業者は業務の取扱中にかかる通信の秘密を侵してはならない。（違反した者は 1 年以下の懲役または 50 万円以下の罰金に処せられます。）

ソフトウェアライセンス
共通編

1. 著作権とは

コンピュータソフトウェア（プログラム）は、著作物の一種として「著作権法」で保護されています。

例えば、小説を執筆したり、音楽を作ったりした場合、その作品はあなたのものとなります。その作品をどのように公表し、どのように修正するかはあなたが決める権利を持ちます。作品が売れた場合は、その見返りはあなたのものとなります。 このような作品にまつわるいろいろな権利を「著作権」と呼びます。 コンピュータソフトウェア（プログラム）は著作権の中に含まれ、勝手にコピーすること、勝手に販売することはその権利を侵害したことになります。

著作権は、英語で「コピーライト（Copyright）」という。その名のとおり、複製（Copy）の活用方法をコントロールする権利（Right）です。著作物は、一般的に複製（コピー）を作って活用することから、その名のとおり複製の活用方法をコントロールする権利です。

2. 代表的な利用条件

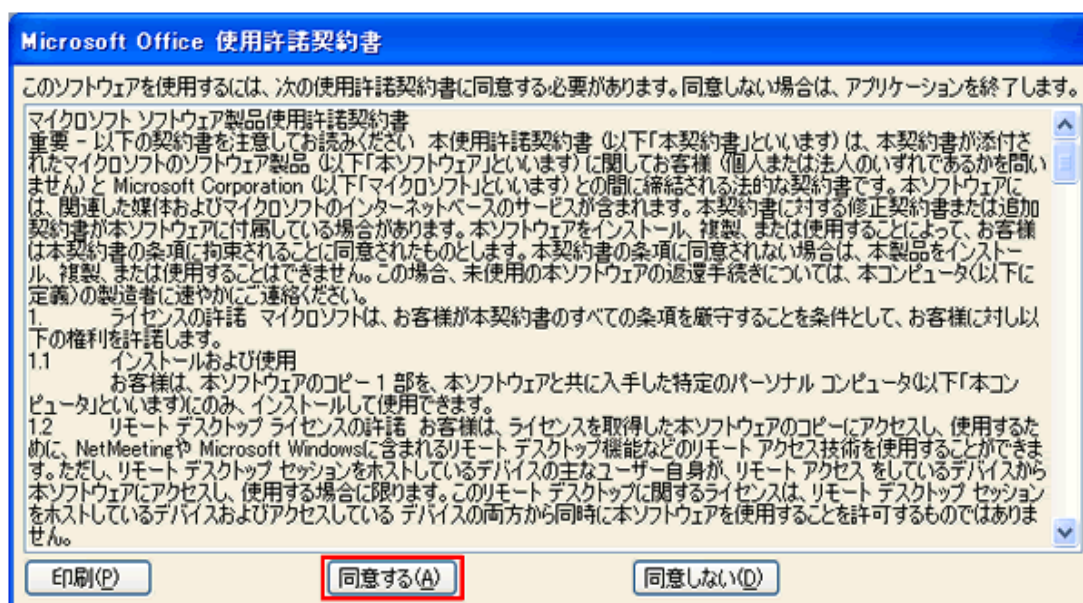
著作物であるソフトウェアを複製したり配布することには、著作権者の許可が必要となります。

Microsoft Office やジャストシステムの一太郎のような市販されているソフトウェアを購入した場合、実は、ソフトウェアのライセンスにお金を払っています。パソコンにプレインストールされているソフトウェアも同様で、パソコン本体価格のなかにライセンス価格が含まれています。 著作物であるソフトウェアを複製したり配布するには、著作権者の許可が必要になります。許可なく勝手に複製して配布することは、通常許可されていません。 友人が所有する Microsoft Excel 等のソフトウェアを、自分のパソコンにインストールするのは、利用条件に反することになります。

利用条件については、複数のタイプがあります。 例えば、企業が社員用のワープロソフトを大量に配布・導入する場合にそなえ、大量複製するための「ボリュームライセンス」を製品とは別に用意している場合が多いです。

3. 使用許諾契約

使用許諾契約は、著作権者による使用の許諾です。

契約に同意することを条件にソフトウェアの使用を許諾されます。

ソフトウェアをパソコンにインストールするときはほとんど、冒頭で「使用許諾契約書」といった画面が表示されます。画面に表示された使用許諾契約書に同意することで、インストール作業を行うことができます。多くの場合、「パソコン 1 台だけにインストール可」、「レンタル禁止」といった内容が表示されています。

4. 使用許諾契約の留意点

使用許諾契約の内容は、同じソフトフェア、同じメーカーの場合でも、ライセンスの種類により異なります。そのため、利用者は使用に先立って、使用許諾契約の内容をしっかりと確認し、契約内容を遵守することが求められます。

例えば、利用条件のなかには、本来ソフトウェアの「使用」にあたる行為を禁じている場合もあります。たとえば、ソフトウェアの動作から内部構造を研究するという「リバースエンジニアリング」は、ソフトウェアの使用として著作権者の許可なく行えるのですが、Microsoft のアプリケーションの利用条件はこれを禁じています。 このように、ライセンスによって利用者の使える範囲を広げると同時に、本来であれば自由に実行できる行為を一部制限する場合があります。

また、アドビシステムの Acrobat や Illustrator では、「バンドル解除の禁止」や「年1回以下の頻度で、有効なライセンスが使用されているかどうか、10 日前に事前通知の後で、チェックを行う権利を有する」といったユニークなものもあります。

5. ソフトウェア入手形態

ソフトウェア入手形態として代表的な、パッケージ、プリインストールソフトウェアを理解しておく必要があります。

■パッケージ

店頭で販売されているソフトウェア製品、または、出来合いの市販ソフトウェア製品のこと。
前者は、CD-ROM やDVDなどのメディアに記録され、マニュアルなどと共に包装されてパソコン専門店などの店頭で販売されているソフトウェア製品の意味です。対義語としては、インターネットなどを通じてダウンロード販売される「オンラインソフト」や、Web ブラウザなどを通じて遠隔利用できる「オンラインアプリケーション」などがあります。後者は、企業の業務用システムなどで出来合いのソフトウェア製品を購入・利用する場合などに使う語です。システム開発会社などに依頼して自社業務に合わせて開発してもらう「オーダーメイドソフト」などと対比する文脈で使われます。

■プリインストール ソフトウエア

コンピュータに OS やよく使うアプリケーション・ソフトウェアが事前にインストールされて提供されているものをプレインストール製品といいます。この製品は、特定のコンピュータでしか使うことができない条件でライセンスが与えられたもので、その使用条件はハードウェアメーカーが決めていますから、メーカーが提供する使用許諾契約内容ををよく読んで、使用範囲を事前に確認する必要があります。

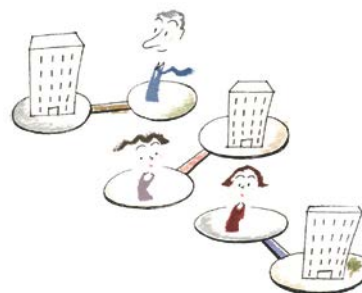
6. ライセンスの種類

ライセンスの種類として最も普及しているのが CPU ライセンスです。また、一般的ではありませんが、高専ではマイクロソフト社との包括ライセンス契約を結んでおり、基本的な内容を理解しておく必要があります。

■CPU ライセンス

インストールして利用できるハードウェアの台数を特定するもので、最も普及している形態です。個人用に市販されている多くのパッケージソフトウェアの使用許諾書では「1 台のコンピュータで使用できます」という趣旨の条項が含まれていますが、この部分が CPU ライセンスであることを示しています。最近では同時に使用しないことを条件に、1 台のデスクトップ型パソコンのほかに、もう 1 台携帯型パソコンであればインストールすることができる、とされている使用許諾契約も増えています。また、1 台用のパッケージを購入するのではなく、複数のコンピュータにインストールして使用できる使用許諾契約を企業や自治体とソフトウェアメーカーの間で直接結ぶケースが多くなっています。1 台用のソフトウェアを複数購入する場合とソフトウェアの使用方法については大きく異なりませんが、パッケージを複数保管しておく必要がないこと、1 台用を複数購入する場合よりもディスカウント価格になっている場合が多いことなどがメリットとされています。

■マイクロソフト包括ライセンス

PC 保有台数ではなく、組織に所属する人数に基づき、ライセンス契約が行われる契約となります。国立高等専門学校機構では、マイクロソフト社と包括ライセンス契約を締結しています。本契約においては、教職員及び学生の人数に基づいて契約を締結していることから、全職員及び全学生が契約内容に含まれます。Windows7、Windows Vista、Windows XP 等のインストールが可能です。
※個人所有のパソコンについてもインストールが可能であり、①学校に PC を持参、②配布システム、③メディア購入の 3 パターンがありますが、詳しくは各校の担当者にお問い合わせ下さい。

7. マイクロソフト包括ライセンス契約

マイクロソフト社と締結している包括ライセンス契約では、個人所有のパソコンにインストールすることが可能ですが、本人だけの使用が条件となります。

国立高等専門学校機構では、マイクロソフト社と包括ライセンス契約を締結しており、全教職員（非常勤職員含む）及び在籍する全学生（本科及び専攻科）が利用可能です。 本契約に基づき、下記が利用可能なパソコンとなります。

【個人所有パソコン】

個人所有のパソコンへは、1 人 1 台のみで次の条件のもとインストールすることができます。

- ◆ 個人所有パソコンへインストールした場合、本人だけの使用が条件となります。家族や友人のソフトウェアの使用は認められません。
- ◆ 国立高等専門学校機構とマイクロソフト社の間で締結している包括ライセンス契約を解除した場合、利用資格喪失により、ソフトウェアを削除する義務を負います。
- ◆ 退学で国立高等専門学校機構の学生でなくなった時や退職（他機関への異動も含む）の場合、利用資格喪失により、ソフトウェアを削除する義務を負います。
- ◆ Windows 製品及び Office 製品それぞれ 1 種類 1 人 1 台に限定し、インストールすることができます。
- ◆ 学生が在籍中に個人所有パソコンにインストールしたソフトは、永続的な利用権（卒業時点のバージョンを永続的に）が与えられますが、卒業時に「学生使用許諾証明書」を国立高等専門学校機構から受け取ることで、そのソフトウェアを永続的に利用することが認められます。

8. マイクロソフト包括ライセンス Q&A

Q1 OS 無しの PC に包括ライセンスの Windows をインストールすることは出来ますか？

A1 包括ライセンスはアップグレード専用につき不可です。

Q2 包括ライセンスの Windows や Office の利用可能なライセンス数を教えて下さい。

A2 学内での利用可能数は無制限ですがアップグレードのみとなります。学外での利用は一人一ライセンスまでです。

Q3 退学前に取得した包括ライセンスは退学後も使用できるか？

A3 できません。

Q4 卒業後に包括ライセンスを取得することは出来るか？

A4 できません。

Q5 卒業前に取得した包括ライセンスは卒業後も使用できるか？

A5 可能です。ただしバージョンアップはできません。

Q6 包括ライセンス Windows の元となる Windows のライセンスで注意する点は？

A6 パッケージ版 Windows の場合、インストールする PC を自由に選べます。PC が故障時への対応に優れています。
DSP 版 Windows の場合、バンドルされたデバイスを利用する限りにおいて PC が自由に選べます。プリインストール版 Windows の場合、その PC でしか利用できません。

**Q7 包括ライセンスで Office(Mac 用)を取得しました。
別に Office(Windows 用)を取得出来ますか？**

A7 できません。

9. 不正コピー

不正コピーとは権利者の使用許諾条件に違反してソフトウェアを複製、もしくはコンピュータに導入(インストール)することです。

■不正コピーとは

不正コピーとは、一般のパッケージの場合、以下となります。
ソフトウェアのインストール数（複製数）＞ライセンス数（複製して使用することを許諾された数）

不正コピーの類型

不正コピーの類型は以下の 5 つがあります。 すべて犯罪になります。

- ◆ 組織内不正コピー
- ◆ 海賊版・偽造版
- ◆ 販売店による不正インストール
- ◆ インターネット・パイラシー（piracy：著作権侵害）
- ◆ ソフトウェアレンタル

■組織内不正コピー

1 台のコンピュータでのみ使用が許諾されたソフトウェアのパッケージを入手して、複数のコンピュータにインストールするというもの。
企業、学校、病院など、複数のコンピュータでソフトウェアを使っている組織内における不正コピー。 現在日本でもっとも多く見られる不正コピー形態です。

■海賊版・偽造版

正規パッケージの無断コピーや、それを真似たものを「海賊版・偽造版」と呼びます。最近では、多くのソフトウェアを 1 枚の CD-ROM に編集した海賊版が海外だけでなく日本国内にも多く出回っています。これら海賊版・偽造版のなかには、コンピュータウィルスなどが混入している非常に危険なコピーがしばしば見られます。

■販売店による違法インストール

販売店が無許諾でソフトウェアをコンピュータにインストールして販売する行為です。こうした違法行為は、ソフトウェア会社のユーザサポートやバージョンアップなどのサービスを受けられないばかりか、違法と知って業務で使用し続けると自らの責任をも問われてしまうなど、多大なリスクがあります。

※購入時、正規のマニュアルやユーザ登録書が提供されないときは、不正インストールの可能性があるので販売店への確認が必要です。

■インターネット・パイラシー（ piracy：著作権侵害）

インターネットへのソフトウェアのアップロードやネット・オークションを利用して海賊版などを郵送する行為です。近年、P2P ファイル交換ソフトを利用した不正コピーが頻繁に見受けられるようになり、毎年国内では数多くの摘発が行われています。
※P2P とは、不特定多数のコンピュータが相互に接続され、直接ファイルなどの情報を送受信するインターネットの利用形態。また、それを可能にするソフトウェアやシステム。

■ソフトウェアレンタル

ソフトウェアメーカーの許諾を得ずに、勝手にソフトウェア・パッケージをレンタルする行為です。違法レンタル店のなかには、コピーツールも同時に提供するなど、ユーザが不正コピーをすることを前提にした悪質な店もあります。また、あらかじめ買い戻す約束をして中古品として販売する「擬似レンタル」も違法行為です。

10. 不正コピーに当たる行為

以下が不正コピーとなります。

■正規品でない海賊版ソフトウェアを入手し、パソコンにインストールすること。

■正規に購入したソフトウェアであっても、認められたインストール可能台数を上回るパソコンにインストールすること。

- ◆ 仕事で急に普段使用しないソフトウェアを使う必要になったため、他のパソコンで使用されているソフトウェアを「すぐにアンインストール（削除）するから大丈夫だろう」と考えインストールした。
- ◆ 新しく購入したパソコンに、今まで使っていたソフトウェアをインストールし直し、古いパソコンのソフトウェアをアンインストールしないまま他部署に回した。
- ◆ 仕事を自宅に持ち帰って行うため、会社で使用しているソフトウェアの CD-ROM を持ち帰り、自宅のパソコンにインストールした。
- ◆ 必要台数分のソフトウェアの購入を申請したところ、予算の都合で購入本数を減らされたが、業務上どうしても必要だったため、ソフトウェアを必要台数分インストールした。
- ◆ パソコンを購入する際、販売代理店の営業マンが、「これはサービスです」と言って、注文していない市販のソフトウェアもインストールしてくれた。しかし、よく確かめてみるとパッケージ（ライセンス）が入っていなかった。
- ◆ 業務で必要なソフトウェアの購入が認められなかったため、インターネットから海賊版ソフトウェアを入手し、インストールした。

出展：「組織内違法コピーの実態を知っていますか」社団法人コンピュータソフトウェア著作権協会（ACCS）

11. 不正コピーのもたらすリスク

不正コピーがもたらすリスクは、大きく、法的責任、ウィルス感染、無保証、の 3 つがあります。

■リスク①:法的責任

不正コピーは、刑事罰、民事責任が伴います。

■リスク②:ウィルス感染

海賊版ディスク、インターネットからのダウンロード、P2P(ファイル共有ソフト)からダウンロードを通しての不正コピーは、ウィルスが広がるルートでもあり、危険が伴います。

■リスク③:無保証

不正コピーは当然、ベンダーからの保証が受けらません。

- ◆ 正常に動かない
- ◆ マニュアルやヘルプもない
- ◆ 技術サポートもない
- ◆ バージョンアップや更新も不可能

12. 教職員等の責務

下記は、ソフトウェア管理規則に定められている「教職員等の責務」です。ソフトウェア管理担当者は、規則を遵守し、ソフトウェアの適切な管理を行う必要があります。

独立行政法人国立高等専門学校機構ソフトウェア管理規則

第15条 教職員等は、ソフトウェア管理について、次の各号に掲げる事項を遵守しなければならない。

- ソフトウェアの購入、インストール、アンインストール、廃棄、譲渡、使用許諾契約の解除及びハードディスクの廃棄等を行おうとする場合は事前に管理担当者に申請すること。
- 管理担当者の承諾なく、機構の所有するソフトウェアのオリジナルディスク及び当該複製物を機構外に持ち出さないこと。
- 管理担当者の承諾なく、個人で所有するソフトウェアを機構の所有するコンピュータにインストールしないこと。
- 管理担当者の承諾に基づき、教職員等が自らコンピュータにソフトウェアをインストール及びアンインストールした場合には、速やかに、当該ソフトウェアを所管する管理担当者に報告すること。

13. 法的責任

私たちが著作権侵害を起こした場合には、刑事罰および民事責任を負うことになります。

■不正コピーを行った場合の刑事罰

コンピュータソフトウェアは著作権法で保護されており、不正コピーは著作権法に違反する行為です。組織ぐるみで不正コピーを行った場合、実際にインストールを行った従業員は 10 年以下の懲役又は 1,000 万円以下の罰金（又はこれれの併科）に処せられる可能性があります。不正コピーを指示した上司や経営者なども、同様の刑事罰を受ける可能性があります。さらに、企業自体も 3 億円以下の罰金刑に処せられる可能性があります。

■不正コピーを行った場合の民事責任

不正コピーを行った場合、その被害を受けたソフトウェアメーカーから、著作権侵害にもとづく損害賠償請求される可能性があります。組織ぐるみで不正コピーを行った場合のみならず、従業員が勝手に不正コピーを行った場合にも、企業には損害賠償を負う責任が生じます。さらに、経営者個人も損害賠償を負う責任が生じる場合があります。

多くの場合は、会社の代理人である弁護士への和解交渉を依頼する費用も発生し、損害賠償を支払っても、必要なソフトウェアは別途することになります。不正コピーは、損害賠償のみならず、多額の損失を組織にもたらします。

	刑事罰（著作権法）	民事責任
企業・ 団体等	3 億円以下の罰金	・組織の意向による不正コピーに対する損害賠償責任 ・上司が知らないところで行われた不正コピーに対する損害賠償責任
代表者	10 年以下の懲役又は 1000 万円以下の罰金（又はこれらの併科）	・代表者が積極的に関与した不正コピーに対する損害賠償責任 ・代表者が従業員の行う不正コピーを放置したことに対する損害賠償責任
従業員	10 年以下の懲役又は 1000 万円以下の罰金（又はこれらの併科）	・従業員が自分の判断で行った不正コピーに対する損害賠償責任

正しく 購入した場合	店頭小売価格		
不正コピーが発覚した場合	店頭小売価格	メーカー希望小売価格×一定の倍率	弁護士費用

出展：「組織内違法コピーの実態を知っていますか」社団法人コンピュータソフトウェア著作権協会（ACCS）

14. 不正コピー裁判事例

司法試験予備校事件

　コンピュータソフトウェアの権利保護を目的とした非営利団体、ビジネス ソフトウェア アライアンス（BusinessSoftware Alliance、以下 BSA、本部：米国ワシントン D.C.、会長：ロバート・W・ハリマン）の会員企業である大手ソフトウェアメーカー3 社が、2000 年 4 月 19 日に大手司法試験予備校である株式会社東京リーガルマインドに対し、コンピュータソフトウェアの組織内での不正コピーによる著作権侵害を理由に、損害賠償を求めていた民事訴訟の判決が、5 月 16 日に東京地方裁判所でありました。東京地裁（飯村敏明裁判長）は、被告企業が、ソフトウェアの組織内不正コピーにより、原告 3 社の著作権を侵害していたことを認める判決を下し、不正コピーが発覚した後に正規品を購入すれば、過去に不正コピーをしていた分についての損害賠償を一切支払う必要はないという被告企業の主張を「失当である」として全面的に否定し、被告である大手司法試験予備校（株）東京リーガルマインドに 8472 万 400 円の損害賠償の支払いを命じました。

　東京地裁は、判決の中で、被告企業による組織内不正コピーによる著作権侵害を以下のように認めました。

　不正コピーが発覚した後に正規品を購入すれば、過去に不正コピーをしていた分についての損害賠償を一切支払う必要はないといった被告企業の主張を「失当である」として全面的に否定し、損害賠償額の算定にあたっては、著作権侵害されたソフトウェア製品の正規品小売価格を算定基準として認め、不正コピーの数についても、1999 年 5 月に被告企業が経営する校舎の一つで行われた証拠保全手続きにおいて検証されたソフトウェアの数以上の不正コピーが行われているとの判断が適用されました。

出展：BSA ホームページリリース記事

不正コピーを指摘されてから購入しても、損害賠償責任は免れません。

不正コピーによる著作権侵害事件は多く存在しますが、学生が逮捕された例として、以下の事件を掲載します。

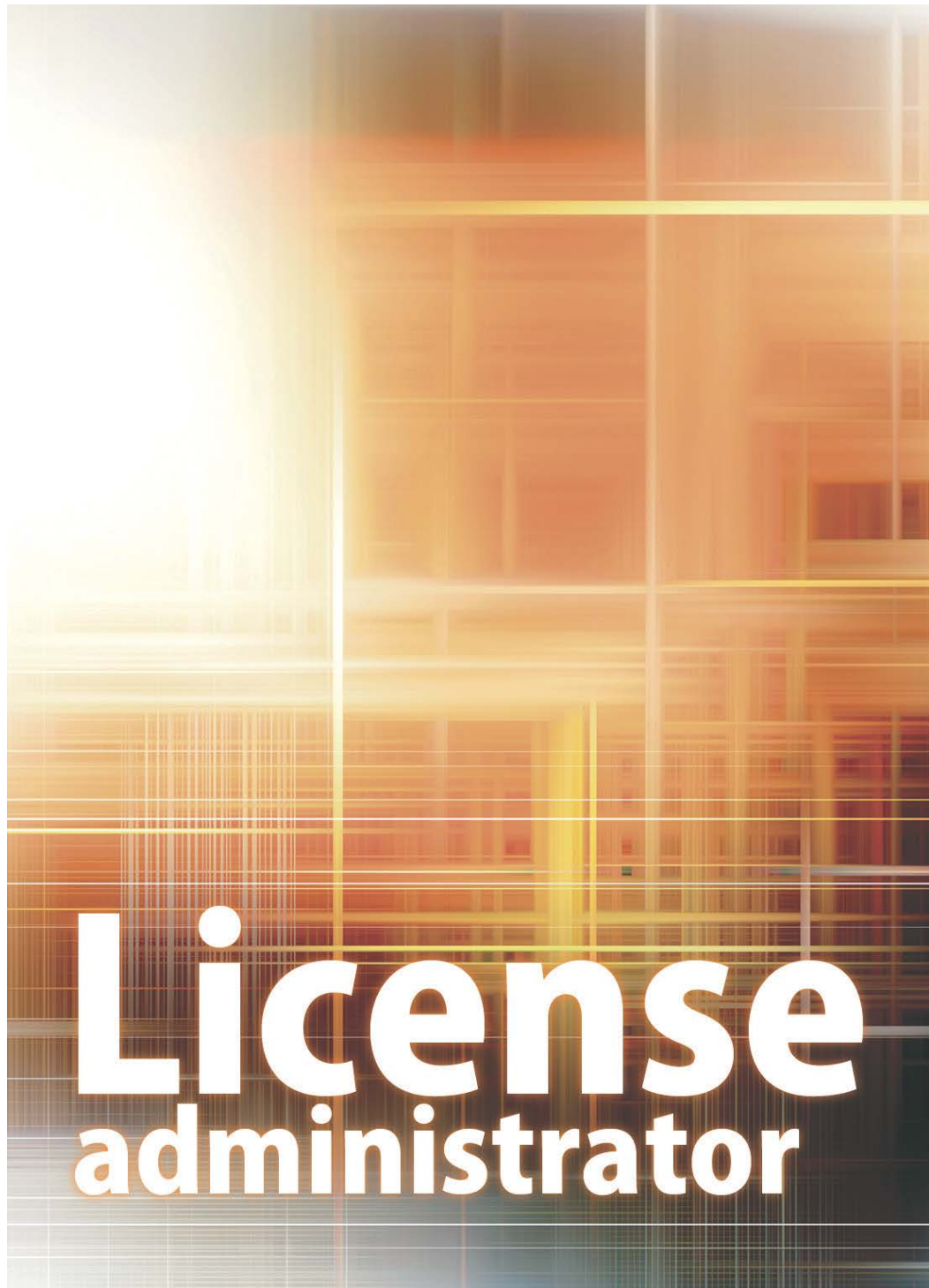
ニュースの内容

警視庁警生活経済課と目白署は、平成 21 年 11 月 2 日、ヤフーオークションを悪用し、権利者に無断で複製したコンピュータソフトを販売していた大阪府富田林市の男子大学生(25 歳)を著作権法違反の疑いで逮捕し、3 日、東京地検に送致しました。

男性は、平成 21 年 8 月 10 日、アドビシステムズインコーポレーティッドが著作権を有する「Adobe Illustrator 10 Windows 版」を権利者に無断で複製した CD-R 1 枚を、東京都の男性に対し販売していました。

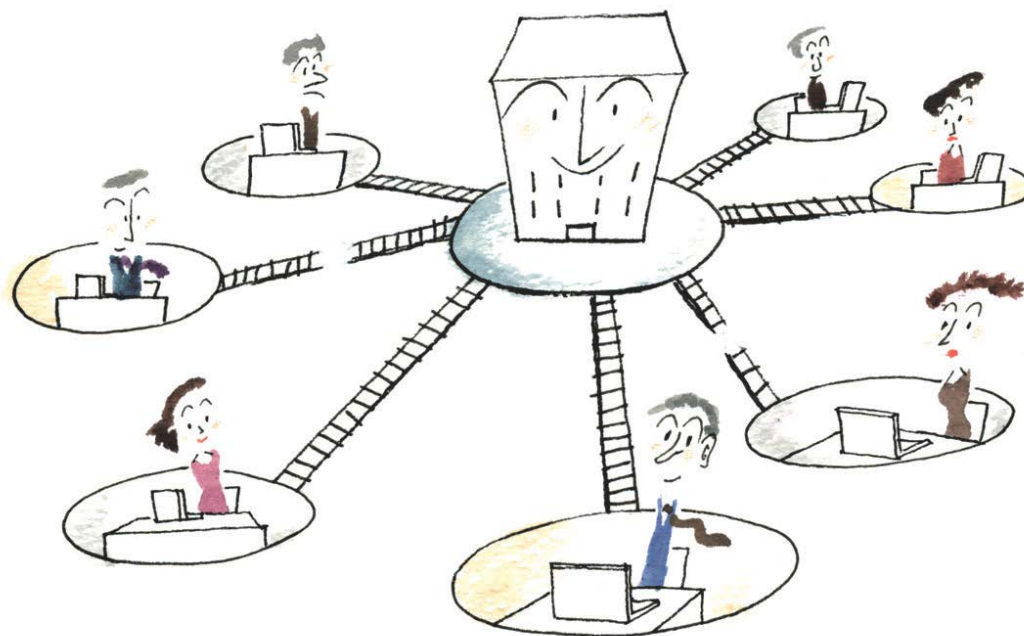
販売の特徴	男性は、「ヤフーオークション」を通じて海賊版を販売していた。 男性は、オークションの出品画面上に「内容はソフトとシリアルのみでユーザ登録は出来ません」と説明していた。
販売価格	男性が 6,000 円で販売していた「Adobe Illustrator 10 Windows 版」の正規品価格は、79,500 円(税別)。
端緒	警視庁の捜査員がサイバーパトロールで男性の出品を発見し、ACCS を通じて著作権者に連絡した。
特記事項	ACCS では、平成 20 年 12 月以降、男性から海賊版ソフトを購入したとみられる落札者の一部が、届いた商品が不正コピーであったことをオークション上の「評価欄」で報告している一方で、「無事にインストールできました。今後も機会があればよろしくお願いします」「この商品についての情報をあらかじめ調べ、納得した上での購入でしたので私は満足しています」など、約 250 件の評価がされていることを確認している。
処分結果	懲役 1 年(執行猶予 3 年)・罰金 30 万円／東京地裁(平成 22 年 1 月 8 日)
鑑定及び告訴	アドビシステムズインコーポレーティッド(アドビシステムズ(株))

出展：ACCS(社団法人コンピュータソフトウェア著作権協会)ホームページ

ソフトウェアライセンス
管理編

1. 使用許諾契約の方式

使用許諾契約の方式は複数のパターンが存在し、管理者はその内容を理解する必要があります。

パッケージに使用許諾契約が同梱され、ソフトウェアの複製物の包装を開披したときや、ユーザが初めてソフトウェアを使用するときに使用許諾契約に同意したとみなすやり方です。

インストール時に契約の内容が表示され、同意することを示すボタンを押したときに契約に同意したと見なすやり方を取るものがあります。

2. 使用許諾契約のチェックポイント

使用許諾契約において、使用できる機器の数は最も重要ですが、それ以外にも利用に関する重要な条件が定められる場合があります。

項　目	説　明
①使用期間	パッケージソフトウェアでは、使用できる期間について特に限定のないことが少なくありませんが、期間の限定がある場合もあります。
②使用できる機器の数	使用できる機器の数を直接指定する例もありますが、次の③④でみるように、使用できる場所や使用できる環境によって指定することもあります。同一の従業員が使用する 2 台目以降のコンピュータにインストールしてよいのかどうかも重要な事項です。
③使用できる場所	使用できる場所、例えば企業のある一事業所に限定する契約があります。その場所にあるコンピュータなら何台でもよいという契約(いわゆるサイトライセンス)と、さらに台数の制限のある契約もあります。
④使用できる環境	使用できる環境を、そのプログラムの動作可能な環境の中でさらに限定する契約もあります。機器のシリアル番号で限定したり、ネットワークに接続されているコンピュータでの使用を禁じたりする例もあります。
⑤改変・翻案のできる範囲	独力でカスタマイズしたり、第三者にカスタマイズを委託したりする予定がある場合には、特に重要な確認項目となります。
⑥公衆送信のできる範囲	社内 LAN で送信することも著作権法上の利用行為の 1 つである公衆送信にあたりますので、社内 LAN を通じて送信することが許されるのかどうかが重要な確認項目となります。
⑦使用できる機器の数	パッケージ・ソフトウェアの契約では、ユーザ企業がさらに第三者に使用させることができる権利 =サブライセンス権が認められることは少ないのですが、交渉を経て締結される大規模導入契約では、子会社や一定の取引先に対してサブライセンスをする権利を規定することがあります。
⑧アップグレード・に関する事項	アップグレードをする場合には、アップグレード版の使用許諾において、旧バージョンの取扱がどのようになるのか、にも注意したほうがよいでしょう。また、社内の使用バージョンを合わせるため等、ダウングレードの必要性が想定される場合には、ダウングレードができるかどうかにも注意が必要です。

3. ソフトウェア管理業務の留意点

ユーザ登録は、メーカーからサポートを受けるためだけでなく、正式なライセンス使用者として、アップグレード情報などを的確にもらうために必要です。

■ユーザ登録

使用許諾契約の締結後、ユーザ登録を行う必要があります。

ユーザ登録は、メーカーからサポートを受けるためだけでなく、正式なライセンス使用者として、アップグレード情報などを的確にもらうためです。

ユーザ登録が、個人名義で行われたために、ソフトウェアが私物化されたり、登録者情報が更新されずにうやむやになったりすることは、少なくありません。こうした事態を避けるためには、ソフトウェアの管理手続きに必ずユーザ登録を含めるようにします。

一般的にソフトウェアの購入を承認したソフトウェア管理担当者を名義人とする場合が多いです。

オリジナルディスクは、ソフトウェア管理担当者にて一括管理する必要があります。

■オリジナルディスクの保管・管理

オリジナルディスクの保管・管理は、組織形態や保管場所の確保などの理由により様々な方法が考えられますが、ソフトウェア管理担当者が一括管理を行い、教職員、学生による勝手なインストールができないよう施錠のうえ管理することが必要です。

ソフトウェア管理担当者が申請された教職員、学生等のパソコンにインストール作業を行うことが望ましいですが、直接行うことが困難な場合、教職員、学生等が適切にインストール作業を行うための体制およびルールの整備が必要になります。

ライセンス証明書やユーザ登録証は、ソフトウェア管理担当者が一括管理し、ファイル保管することが必要です。箱などに明記されている場合や、各部署でオリジナルを保管している場合はそれらをコピーして一括保管する必要があります。

ソフトウェア入手形態	ライセンス管理に必要な証明書類
①パッケージ	○シリアルナンバーなどが記載されたもの ○使用許諾契約書 △ユーザ登録控え（シリアルナンバーなどが記載されたもの）
②ボリュームライセンス契約	○使用許諾契約書などライセンス数が記載されたもの

③バンドルソフトウェア	△ユーザ登録控え（シリアルナンバーなどが記載されたもの）
④プリインストールソフトウェア	○プロダクトキーシールのコピー ※ ○シリアルナンバーなどが記載されたもの ○使用許諾契約書 △ユーザ登録控え（シリアルナンバーなどが記載されたもの） ○取扱説明書やカタログ中のプリインストール・ソフトウェア一覧
⑤シェアウェア	○使用料金控えなど正規に購入したことが分かる書類

○：ライセンス数を確認するために必須
△：○印の証明書類が紛失している場合などに、ライセンス数を確認するための手がかりとなる

出展：「ソフトウェア自主調査ガイド」社団法人コンピュータソフトウェア著作権協会（ACCS）

インストール数がライセンス数を上回ることがないように、管理台帳を日々更新して管理することが必要です。

管理台帳の管理

管理台帳にインストールする予定のソフトウェア（コンピュータ）情報を記入し、ライセンスを割り当てます。その上でコンピュータにソフトウェアをインストールします。

ライセンスの割当とインストール業務を別々の者が行い、ライセンスとインストールの関連づけを２人で照合したほうが管理手続きが厳守され、ライセンスの不正使用が発生しにくくなります。

たとえ一瞬でも、インストールしたソフトウェアが購入したライセンス数を超えてしまうと、不正使用となります。そのため、ソフトウェアのインストール数（複製数）　<　ライセンス数（複製して使用することを許諾された数）の状態を常に維持する必要があります。

組織内のコンピュータにインストールされているソフトウェアは日々の業務の中で変化します。これに伴い、インストール状況の変化をインストール管理台帳に正確・速やかに反映（更新）させることが必要です。

※管理台帳の様式については、[独立行政法人国立高等専門学校機構ソフトウェア管理規則]を参照してください。

ソフトウェア管理者及び担当者は、著作権法その他関連法令及び使用許諾契約書の内容をソフトウェアの使用者に周知する必要があります。

ソフトウェア管理者及び担当者は、著作権法その他関連法令及び使用許諾契約書の内容をソフトウェアの使用者に周知する必要があります。

例えば、学生の卒業時に「学生使用許諾証明書」を国立高等専門学校機構から受け取ることで、そのソフトウェアを永続的に利用することが認められる包括ライセンス契約は特異な内容です。学生使用許諾証明書を渡すことで初めて、ライセンスの権利を有します。

ソフトウェア管理者は、教職員、学生等が適切な使用を行うよう、周知に努めなければなりません。

4. 情報セキュリティ関連規程

ソフトウェアライセンス管理においては、情報セキュリティ関連規程との関係も把握しておく必要があります。

（1）情報セキュリティ管理規程

（規程・手順等の整備）

第8条　情報セキュリティ責任者は、情報セキュリティ推進責任者の協力の下で、本校の情報システムの利用について次の各号に掲げる場合に対応する規程又は手順等を整備するものとする。

六　業務従事者が、新たにソフトウェアを購入又は借用しインストールして利用する場合並びにインストールを解除する場合

（2）情報セキュリティ推進規程

（コンピュータシステムに関する対策）

第7条　情報セキュリティ推進責任者は、コンピュータシステムを設置する場合に、別に定める「コンピュータシステムの情報セキュリティ対策実施手順」に従ってコンピュータシステムを設定し運用するとともに、次の各号に掲げる措置を講ずるものとする。

二　利用を許可するソフトウェアを定めること。ただし、利用を許可するソフトウェアの列挙が困難な場合には、利用を許可しないソフトウェアの列挙、又は両者の併用でこれに代えることができる。

（3）情報セキュリティ教職員規程

（機構が扱う情報及び本校の情報システムの利用に係わる禁止事項）

第8条　本校の教職員は、機構が扱う情報及び本校の情報システムについて、次の各号に掲げる行為を行ってはならない。

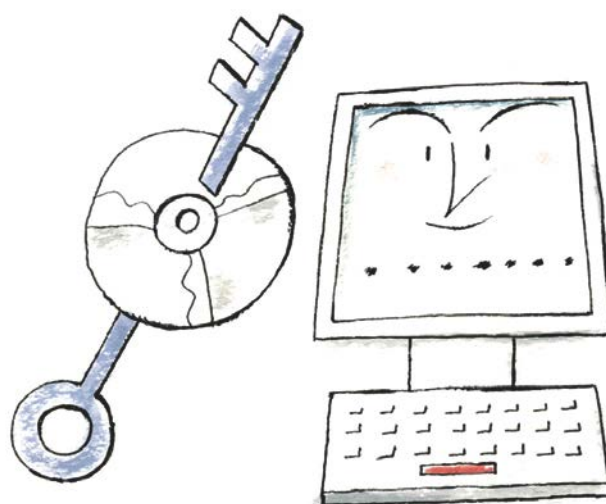
三　情報セキュリティ推進責任者の許可を得ずに、新たにソフトウェアインストールすること及びコンピュータの設定の変更を行うこと。ただし、オープンソースソフトウェアについては「 PC 取扱ガイドライン」によるものとする。

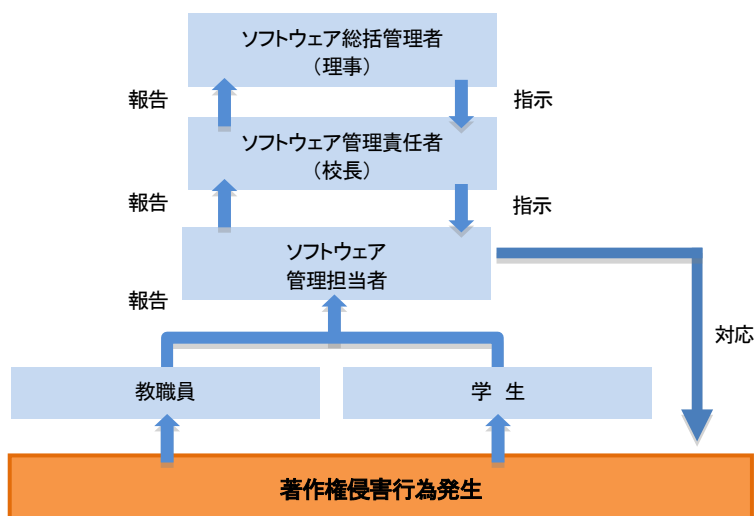
（本校支給以外の情報システムからの利用及び本校支給以外の情報システムの持込）

第19条

五　当該情報システムで動作するソフトウェアがすべて正規のライセンスを受けたものであることを確認すること。

（情報システムの導入）

第20条 本校の教職員が新たにソフトウェアを購入又は借用し自己の管理するPCにインストールして利用しようとする場合は、事前に情報セキュリティ推進責任者に届出るとともに、「情報システム導入手順」に従って必要な措置を講じなければならない。

5. 著作権を侵害する行為への対応について

著作権を侵害する行為が発覚した場合、速やかに上位責任者へ報告を行うとともにその対応を実施しなければなりません。

「独立行政法人国立高等専門学校機構ソフトウェア管理規則」に基づき、著作権を侵害する行為が発覚した場合、以下の流れで対応しなければなりません。

- ソフトフェア管担当者は、著作権侵害に関する行為を教職員、学生から報告を受けた場合、直ちにソフトウェア管理責任者に報告を行わなければなりません。
- ソフトウェア管理責任者は、ソフトウェア管理担当者から報告を受けた場合、直ちにソフトウェア総括管理者に報告するとともに、その対応指示を受けます。
- ソフトウェア管理責任者はソフトウェア総括管理者の指示に従うとともに、ソフトウェア管理担当者に指示を行わなければなりません。
- ソフトウェア管理担当者は、ソフト管理責任者からの指示に基づき、速やかに対応しなければなりません。

ソフトウェアライセンス
参考資料

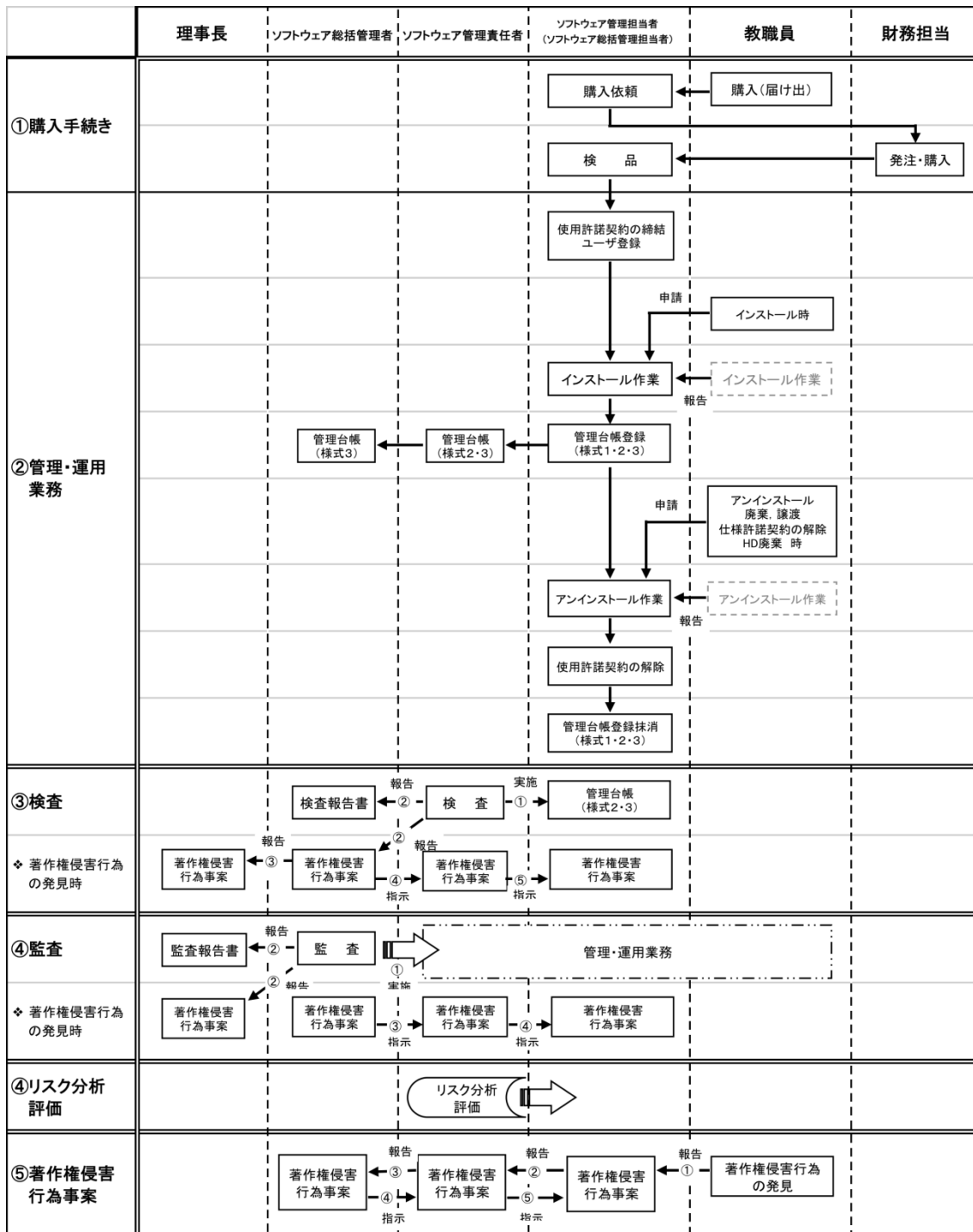
1. ライセンスの種類

主なソフトウェアライセンスの種類として、以下のようなものが挙げられます。

ライセンスの種類	概要説明
CPU ライセンス	インストールして利用できるハードウェアの台数を特定するもので、最も普及している形態です。個人用に市販されている多くのパッケージソフトウェアの使用許諾書では「1 台のコンピュータで使用できます」という趣旨の条項が含まれていますが、この部分が CPU ライセンスであることを示しています。最近では同時に使用しないことを条件に、1 台のデスクトップ型パソコンのほかに、もう 1 台携帯型パソコンであればインストールすることができる、とされている使用許諾契約も増えています。 またボリュームライセンスという形式で、1 枚の CD-ROM にシリアルナンバーなどの認証方式を多数付与し、数十台、数百台のパソコンにソフトウェアをインストールできるような契約内容になっているものもあります。1 ライセンス当たりの料金は通常のパッケージ販売に比べて安くなるのが普通です。必要に応じてライセンスを追加することが可能である場合も多いです。ボリュームライセンスは、企業や学校、官公庁などにおいて採用されることが多く、オペレーティングシステム（OS）の Windows や Mac OS、オフィススイートの Microsoft Office などをはじめ、様々な製品がボリュームライセンスの形式で提供されています。 その他の形式としては、1 つのライセンスで 1 台のマシンへのインストールを許可する、マシン固定ライセンスといったものもあります。
ユーザーライセンス	ハードウェアの特定ではなく、ソフトウェアの使用者の方を特定するものです。例えば、3 人の使用が認められる契約を結んでいる場合には、インストールするコンピュータの台数は制限されず、特定の 3 人ならば使用が認められます。ユーザーライセンスは、電子メールソフトウェアなど特定のユーザーがその人固有の環境で使うソフトウェアで多く利用されている形態です。 独立行政法人国立高等専門学校機構がマイクロソフト社と締結している包括ライセンス契約は、ユーザーライセンスに含まれます。 また 1 つのライセンスで特定の 1 ユーザによる利用を許可するライセンスとして、ユーザー固定ライセンスといった形式もあります。
サイトライセンス	特定のサイト（学校やオフィスなど）に存在するコンピュータについて包括的にインストールして使用できる権限を与える形態です。この契約を結べば、そのサイトに存在している限り何台でも誰でもインストールして使用することができます。大量にソフトウェアを購入する大企業などで採用されている契約形態です。
サーバライセンス	LAN を導入している場合に、特定のサーバへのインストールとそのサーバに接続しているクライアントコンピュータでのソフトウェアの使用が認められる形態です。ネットワーク OS やメーリングソフトウェアなどで見られる形態です。
同時使用ライセンス	同時にソフトウェアを使用できる数を制限する形態です。インストールするハードウェアの台数や使用者の人数に制限はありません。例えば、10 台のコンピュータを 8 人で利用しているときに、この形態で 5 台での同時使用が認められている契約を締結していた場合、10 台全てのコンピュータにそのソフトウェアをインストールすることができ、全員がそれを使用することができるのですが、同時には 5 台までしか使用できないことになります。この契約形態は、「全員に必要だが、全員が毎日使うわけではない」ようなソフトウェアなどの使用に適していると言われています。

2. ソフトウェア入手形態

ソフトウェア入手形態	概要説明
パッケージ	店頭で販売されているソフトウェア製品、または、出来合いの市販ソフトウェア製品のこと。前者は、CD-ROM や DVD などのメディアに記録され、マニュアルなどと共に包装されてパソコン専門店などの店頭で販売されているソフトウェア製品の意味である。対義語としては、インターネットなどを通じてダウンロード販売される「オンラインソフト」や、Web ブラウザなどを通じて遠隔利用できる「オンラインアプリケーション」などがあります。 後者は、企業の業務用システムなどで出来合いのソフトウェア製品を購入・利用する場合などに使う語です。システム開発会社などに依頼して自社業務に合わせて開発してもらう「オーダーメイドソフト」などと対比する文脈で使われます。
バンドル ソフトウェア	デジタルカメラやプリンターなどの周辺機器を購入すると使用するために必要な設定プログラムとは別に、その周辺機器を利用する上で便利なソフトウェアが同梱されていることがあります。これらをバンドルソフトウェアと呼びます。当該周辺機器の使用者に対し、1 台のコンピュータにインストールして使用することが許諾されているものも多くありますので、使用許諾契約を必ず確認する必要がある。 また、コンピュータを購入した際にインストールはされていないが同梱されているソフトウェアをさすこともあります。
プリインストール ソフトウェア	コンピュータに OS やよく使うアプリケーション・ソフトウェアが事前にインストールされて提供されているものをプレインストール製品といいます。 このプレインストール製品は、特定のコンピュータでしか使うことができない条件でライセンスが与えられたもので、その使用条件はハードウェアメーカーが決めていますから、メーカーが提供する使用許諾契約内容をよく読んで、使用範囲を事前に確認する必要がある。
シェアウェア	ソフトウェアの流通形態の一つ。ユーザはネットワークなどから自由にソフトウェアを取得することができ、一定の試用期間の間は料金を払わずに利用することができる(試用版には制限が設けられていることもある)。試用してみて気に入ったら、入金してユーザ登録を行い、継続利用する権利を取得する。

3. ソフトウェア管理業務に関するフローチャート

4. ソフトウェアライセンスの理解を助ける情報提供サイト集

ソフトウェアライセンスをより理解するために、参考情報として、情報提供サイトのリンク集を掲載します。

◆ 「ソフトウェア資産管理基準」（ソフトウェア資産管理コンソーシアム）
http://www.samconsortium.org/act.html

◆ 「ソフトウェア管理マニュアル」（社団法人コンピュータソフトウェア著作権協会）
http://www2.accsjp.or.jp/sam/download.php

◆ 「サンプル書式集」（マイクロソフト株式会社）
http://www.microsoft.com/japan/education/license/hokatsu/faq.mspx

◆ 「著作権侵害事件」（社団法人コンピュータソフトウェア著作権協会）
http://www2.accsjp.or.jp/criminal/

索　引

あ

か

さ

情報システムユーザガイドライン

発行日：平成２３年６月 初版
平成２５年９月 第２版
編　集：情報基盤委員会
情報基盤整備専門部会
情報セキュリティ専門部会
ＩＴ研修専門部会